MODERN ALGEBRA

FOR
HONOURS AND POST-GRADUATE STUDENTS
OF
All Indian Universities and for various Competitive Examinations

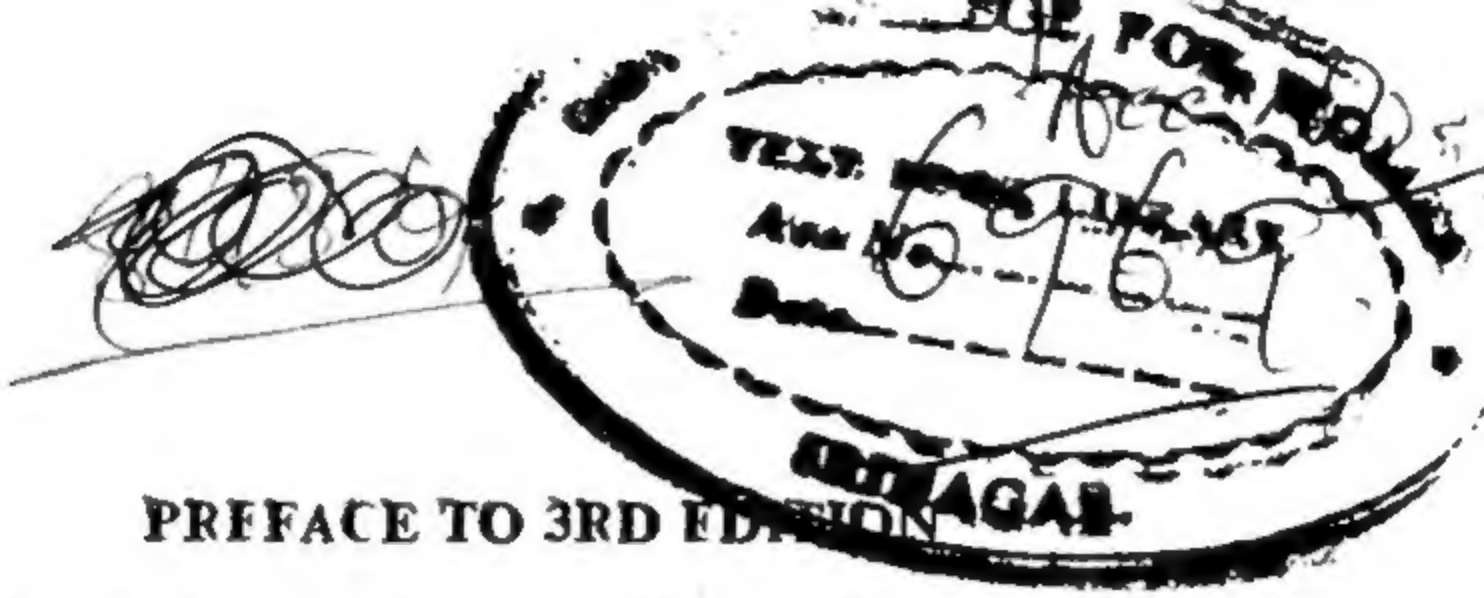
483-M.L.K.

Math

by

M. L. Khanna

JAI PRAKASH NATH & Co.,
PUBLISHERS — MEERUT-2



PREFACE TO 3RD EDITION

The book has undergone thorough revision with the result that there are many additions which has again increased the volume of the book. List of important questions and articles have been given at the end of each chapter and there deserve special attention from the students.

Great care has been taken that the book is free from printing mistakes.

Any suggestion for improvement of the book will be thankfully received.

'Vijay'
Saket Road, Meerut
Phone 2217

M. L. KHANNA

Author

3, **An Important note.**

There are two books titled as Modern Algebra, one is for degree classes and the other for Hon's and Post graduate classes.

Modern Algebra for degree classes. Contains the matter upto page 400 of the contents which cover the topics Groups, sub groups. Rings, and Vector spaces.

Modern Algebra for Hon's and Post graduate classes. Contains 482 pages which cover the topics, "Groups. Rings, Vector spaces, Normal sub groups. Group homomorphism, Quotient ring and ring homomorphism and Euclidean domain". You will please choose the book which covers your syllabus.

PREFACE TO THE FIRST EDITION

The present book is meant for Hon's. and post graduate students of all Indian Universities and particularly for students of Meerut University.

The treatment of the theory which is a special feature of the book is in a systematic and interesting manner. Even an average student shall be able to understand it independently.

Large number of solved examples have been given to make clear the various definitions and theorems.

It is easy to understand the subject matter but may be difficult to reproduce the same independently and as such the students are advised to adopt pen and paper for its study.

Any suggestion for improvement of the book will be thankfully received.

M. L. KHANNA

PREFACE TO SECOND EDITION

The subject matter has been thoroughly revised which has resulted in the increase of the volume of the book by about 200 pages. Many new questions and additional theorems have been added. The book in its present form will meet the requirements of students of all Indian Universities.

'Vijay'
Saket Road, Meerut
Phone 2217

M. L. KHANNA

"DONT READ THIS"

1. Never Read Mathmatics. Always adopt pen and paper for doing mathematics otherwise you will be simply deceiving yourself. You will never be able to reproduce the solution of a question in the examination unless or until you have done it earlier in writing.

2. University Papers. To create in your the confidence the best method is that after you have done one chapter or more chapters, turn to the university papers given in the end and do the questions of these chapters independently and in case you are able to do them, then and only then you should feel confident of doing well in the examination.

3. Selection. There is no harm in making a selection of books. (*i.e.* Diff., Coordinate, Trigonometry etc.) which you are going to prepare or even selection of chapters of any of these books. But whatever you decide to prepare, you should prepare it very thoroughly. Do all types of questions, **Do not make a selection out of the selection,** otherwise you will always suffer with a lack of confidence. Remember

"Better know everything of something.
Rather than something of everything.
and
Nothing like if you know everything of everything."

Pay special attention to the questions and articles given in the list of important questions at the end of each chapter.

4. Revision before examination. In order to simplify the work of revision before examination, you should while preparing any book or its chapter, mark "R" with **red ink** in your copy those questions which you feel are difficult or require some special trick or method and which you are likely to forget. Only these questions may be looked and revised the day before the examination. Do not include in this list those type of questions which are based upon direct application of formula and which you can always do.

5. Important formulae. There are certain basic and standard formulae of various branches of mathematics which every student is expected to know, but it is found that the students are not definite about these standard results of

Trigonometry. Differential and Integral Calculus. Coordinate Geometry etc. You are therefore advised to leave a small margin in your copy and write in it the formula about which you are not sure and which is reqired for the solution of that particular problem. This will demarcate what you know and what you do not know and will facilitate the work of revision also

6. Before going to your class. In order to draw the maximum benefit out of this book, you should always before going to your class read the portion of this book which your teacher is going to discuss in the class. This will create greater interest in the lecture. You can also clear some point from your teacher which you might not have been able to understand independently from my book.

7. Regularity in Study of Mathematics The most important thing in the study of mathematics is regularity in its studies. You should see that you are working regularly with the class and do not postpone your daily work of mathematics.

8. In the examination. Avoid over-writing and scratching in the copy. Look to the note given in the paper and attempt first the question which you know well. Attempt maximum number of questions. Always revise your answers. Keep left side of the page for rough work and cross it.

9. Correspondence with the author. You are most welcome to correspond with me with regard to any suggestions alternative solutions of questions, new questions which you like to be incorporated, or your difficulty with regard to any question from this book alone, or to point out the printing mistakes which you may come across.

10. On expectation In case you have liked this book or some other books of mine and found them really helpful to you, I would certainly desire and expect that you will recommend them to your class-fellows.

M. L. KHANNA
'Vijay' Saket Road, Meerut.

MUST READ THIS

PUBLISHER'S NOTE

We are very much proud in presenting our Mathematics series written by Prof, M. L. Khanna, who has all through his college carrer been a first class student a position and merit scholarship holder. The present B. Sc. series is the result of many years of hard labour put in by the author and each book of the series serves the **triple purpose of (i) Text book, (ii) Help Book, and (iii) University Papers, and is thus much economical. In addition to this, since each book of the series is written by the same author. you can be sure of the uniformity of expression and style in all the 50 books of Prof. Khanna that have been published so far. In case you want to purchase any new book of mathematics, you are very sincerely advised in you own interest to look to the Author's book on the subject. Borrow it from a friend for few days and you will find it for yourself that these books really serve the triple purpose and in case you are having it you need not supplement it by any other book. You are further advised to gain by the experience and opinions given before and expressed by various heads of the department and lecturers of Mathematics from different places. In the end it gives us immense pleasure to inform you that if you turn to the university papers in the end you will find that practically cent per cent questions were set from the author's books in various university examinations.**

The publishers will feel highly obliged for any suggestions for improvement of the books.

V. N. GUPTA

for

Jai Prakash Nath & Co.

Where is What

List of Formulae XVI—XXIV

Chap. I. Groups. 1—128

§ 1. Binary Composition. 1

§ 2. Various Types of Compositions. 3

§ 3. Group (Definition). 6

Examples of groups. Exercise I. 8

§ 4. Addition and multiplication modulo m. 32

§ 5. Residue classes modulo m 41

Th. Residue classes modulo m form a finite group w.r.t, addition of residue classes. 43

Th. No n zero residue classes modulo m (m composite integer) do not form a group w.r.t. multiplication of residue classes but when m is prime then they form a group. 44

§ 6 General properties of groups. 45

Left Cancellation Law, Left identity is right identity, Left inverse is Right inverse, Right Cancellation Law. Unique solution of equations $ax=b$, $ya=b$. Identity element is unique Inverse of an element is unique $(a^{-1})^{-1}=a$, Reversal law for inverse. An alternate definition of a group.

Th. Criteria for a finite set G to be a group. 51

§ 6(a) Permutations. 53

Th. The n ! permutations form a group w. r. t. permutation multiplication. 57

§ 7. Cyclic permutation. 60

Expression for any permutation in terms of cycles. 61

		Pages
	Examples.	63
§ 9.	Transposition.	65
Th.	If permutation P can be expressed as the product of r and also of s transpositions then either both r and s are even or both odd.	67
§ 10.	Of the n ! permutations on n symbols, $\frac{1}{2}(n)$! are even and $\frac{1}{2}(n)$! are odd.	70
	$\frac{1}{2}(n)$! even permutations form a finite non abelian group w.r.t. permutation multiplication.	71
	Examples.	73
§ 11.	Integrals powers of an element of a group.	78
§ 12.	Order of an element of a group.	79
§ 13.	Certain Theorems on the order of an element of a group.	81
	Exercise 4	84
§ 14.	General Law of commutativity of the elements of a group.	91
§ 15.	One-one onto mapping preserving group composition.	92
§ 16.	Isomorphism of groups.	94
	Exercise 5	95
§ 17.	Important properties of Isomorphic mappings.	103
Th.	The relation of Isomorphism in the set of all groups is an equivalence relation.	110
§ 18.	Transference of group structure.	112
Th.	Cayley's Theorem ; Every finite group G is isomorphic to a permutation group.	114
	Exercise 6	117
§ 19.	Cyclic groups.	120
	Exercise 7.	121

		Pages
	Certain Theorems on Cyclic groups.	123
	List of important questions and articles.	128
Chap. II.	**Sub groups.**	129—167
§ 1.	Sub groups.	129
§ 2.	The identity, inverse and order of an element of a sub group.	130
§ 3.	Criteria for a sub group. Theorems.	131
	Exercise I.	136
§ 4.	Intersection of two sub groups of a group G is again a sub group of G. Theorem.	140
§ 5.	Union of two sub groups. Theorem	141
§ 6.	Algebra of complexes of a group. Theorems	142
§ 7.	Sub group of a cyclic group (Theorems)	146
§ 8.	Cosets.	148
	Exercise 2.	149
§ 9.	Theorems on Cosets.	151
	Exercise 3.	154
§ 10.	Coset Decomposition	159
§ 11.	Lagrange's Theorem : The order of a sub-group H of a finite group G is a divisor of the order of the group G.	161
	Every Group of prime order p is cyclic.	163
	List important questions and articles.	167
Chap. III.	**Rings, Integral domain, Fields, polynomial rings.**	168—282
§ 1.	Ring (Definition).	168
	Examples on rings. Exercise I.	169
§ 2.	General properties of rings.	176
§ 3.	Types of rings	177
	Commutative ring, Ring with unity, Rings with	

		Pages
	zero divisors, Rings without zero divisors.	178
	Exercise 2.	180
§ 4.	Cancellation Law in a ring, Th. 1.	191
§ 5.	Integral domain.	192
§ 6.	Field.	195
	Exercise 3.	196
§ 7_s	Certain Theorem on Fields. Th. 2—5.	204
§ 8.	Division ring or a skew field.	209
§ 9.	Isomorphism of two rings.	210
§ 10.	Theorem on isomorphism of rings. Theorems *A*, *B*, *C*, *D*, *E*, *F*, *G*, *H*	211
	The relation of isomorphism in the set of all rings is an equivalence relation.	213
§ 11.	Transference of ring structure.	218
§ 12.	Sub rings.	218
§ 13.	Theorem on sub rings. Th. 7—9	221
	Exercies 4.	223
§ 14.	Sub Field.	224
§ 15.	Ordered integral domain.	225
	Exercise 5.	227
§ 16.	Divisibility in an integral domain.	
§ 17.	Units and associates in an integral domain. Th. 12—13.	228
§ 18.	Characteristic of a ring. Th. 14—16.	231
§ 19.	Quotient field of an integral domain.	236
§ 20.	Ideals.	245
	Exercise 6.	247
§ 21.	Certain Theorem on Ideals. Th. 19—21.	250
§ 22.	Smallest left ideal containing a given sub set *S*.	253
	Exercise 7.	253
§ 23.	Principal Ideal.	256

		Pages
§ 24.	Principal Ideal ring.	257
	Excercise 8.	258
Th.	Ring of integers is a principal ideal ring.	260
§ 25.	Maximal Ideal	261
§ 26.	Polynomial rings.	263
§ 27.	Isomorphism of a set of constant polynomials of $R[x]$ on R.	266
Th.	The set of all polynomials over a ring R forms a ring w. r. t. addition and multiplication of polynomials.	267
§ 28.	If R is an integral domain so is $R[x]$.	268
	Theorems.	269
§ 29.	Divisibility of polynomials over a field.	270
§ 30.	Division Algorithm for polynomials over a field F.	272
§ 31.	Remainder Theorem.	274
§ 32.	Synthetic Divison.	276
§ 33.	Greatest common Divisor	280
§ 34.	Euclidean Algorithm for polynomials over a field.	280
List of important questions and articles,		282
Chapter IV Vector Spaces.		283—400
§ 1.	Introduction.	283
§ 2.	Vector space over a field F (definition).	285
	Exercise 1.	286
§ 3	Properties of vector space.	296
§ 4.	Vector sub space.	298
§ 6.	Criteria for a sub space.	298
	Intersection of two sub spaces is a sub space.	301
§ 6.	Linear sum of two sub spaces. Th. 5.	303

	Pages
§7. Direct sum of two sub spaces.	304
Th. 6. *Critetia for direct sum.*	306
Exercise 2,	308
§ 8. Linear combination of Vectors.	313
§ 9. Linear span of a set. Th. 7, 8.	314
§ 10. Linear Dependence and Independence.	319
Exercise 4.	322
Th. 9. Theorem on Linear Dependence.	328
§ 11. Bases.	329
Exercise no. 5	329
§ 12. Finite dimensional vector space	335
Theorem on basis of a f. d. Vector space. Existence and invariance Theorems.	337
§ 13. Dimensions of a vector space.	340
Th. 12. Extension Theorem.	340
Th. 13. Dimension of a sub space.	344
Th. 14. Dimension of direct sum.	345
Th. 16. Existence of Supplementary sub space.	347
Th. 17. Dimension of Linear sum.	349
§ 14. Quotient space.	351
Th. 18. The set V/W of all cosets is a Vector space.	353
Th. 19. Dimension of quotient space V/W.	355
§ 15. Vector space homomorphism	357
§ 16. Properties of homomorphism.	358
§ 17. Vector space Isomorphism.	360
Exercise 5	360
Th. 20. Every n dimensional vector space V (F) is isomorphic to V_n (F).	363
Th. 21. U (F) $\cong$ V (F) $\Leftrightarrow$ dim U = dim V.	364

		Pages
	Excercise. 6	367
§ 18.	Linear transformations,	372
Th. 24.	Vector space of linear transformations.	376
§ 19.	Composite transformations.	378
§ 20.	Composite linear operator	380
§ 21.	Properties of multiplication of linear operators	382
§ 22.	Algebra.	383
§ 23.	Linear functionals on a vector space,	386
§ 24.	Dual space of a vector space.	389
§ 25.	Dimension of duel space.	394
List of important questions and articles.		400
Note.	The matter beyond P. 400 is contained only in the book "Modern Algebra for M.Sc. and Hon's."	
Chap. V.	**Normal Sub groups**	401–430
§ 1.	Introduction.	401
§ 2.	Normal sub group. Definition.	401
§ 3.	Different characterisation of normal sub groups. Th. 1, Th. 2, Th. 3	402
Th. 4.	Intersection of two normal sub groups.	406
	Exercise 1.	407
§ 4.	Simple group.	415
§ 5.	Relation of conjugacy in a group G.	415
§ 6.	Normalizer of an element of a group.	417
	Theorem on normalizer	418
§ 7.	Self conjugate elements.	421
§ 8.	Centre of a group.	421
	Theorems.	422
§ 9.	Conjugate sub group.	423
Th. 10.	The relation of conjugacy is an equivalence relation in the set of all sub groups of a group G.	

		Pages
§ 10.	Quotient groups. Th. 12.	424
§ 11.	Sub groups generated by a sub set of a group.	427
§ 12	Commutator sub group of a group Th. 14.	428
Chap. VI	**Group Homomorphism**	431–454
§ 1.	Homomorphism onto, into, Endomorphism.	431
§ 2.	Properties of homomorphism.	432
§ 3.	Kernel of homomorphism.	433
	Th. 1, 2, 3, 4	334
Th. 4.	Every quotient group of a given group G is a homomorphic image of the group. The kernel of f is H.	435
Th. 5.	Every homomorphic image G′ of a group is a isomorphic to some quotient group there of. Exercise I.	436
§ 4.	Automorphism of groups.	442
Th. 6.	The set of all automorphism of a group forms a group w. r. t. composite of functions as the the composition.	443
§ 5.	Inner automorphism, Th. 7.	446
Th. 8.	Group of Inner automorphism.	447
§ 6.	External direct products.	450
	Theorem, 9, 10, 11	451
Chapter VI.	**Quolient ring and ring homomorphism.**	455–469
§ 1.	Quotient ring	455
§ 2.	Ring homomorphism.	461
§ 3.	Certain properties of ring homomorphism	462
§ 4.	Kernel of ring homomorphism.	464
Th. 3.	Kernel of homomoephism of a ring is a two sided ideal.	465

Th. 4. Every quotient ring of a given ring R is a homomorphic image of the ring. 464

Th. 5. Every homomorphic image R' of a ring R is isomorphic to some quotient ring there of. 465

Chapter VII. Euclidean Domain. 469–482

§ 1. Definition. 469

Excercise 3.

Th. 1. Every euclidean domain is a principal ideal domain. 474

Th. 2. Every euclidean domain possesses unity element. 475

§ 2. Greatest Common Divisor. 475

Th. 3. Existence of greatest common divisor 476

§ 3. Relatively prime elements of euclidean domain 477

Certain Theorem 4, 5, 6, 7. 478

§ 4. Unique factorization Theorem in an Euclidean domain. 480

LISTS OF IMPORTANT FORMULAE

Groups

1. Binary Composition. If G be a non empty set and $a, b \in G$, then a composition denoted as o such that $a\ o\ b \in G$ is called a binary composition on the set G.

2. Group : A non empty set G with a binary composition o, such that

G_1 **The composition is associative :**

i.e., $(a\ o\ b)\ o\ c = a\ o\ (b\ o\ c)\ \forall\ a, b, c \in G.$

G_2 **Identity :** $\forall\ a \in G$ there exists unique element $e \in G$ such that $a\ o\ e = e\ o\ a = a$

G_3 **Inverse :** $\forall\ a \in G$ there exists an element $b \in G$, such that $a\ o\ b = b\ o\ a = e$

In case the composition in G is commutative, *i.e.* $a\ o\ b = b\ o\ a$, $\forall\ a, b \in G$ then the above group is called abelian.

3. General properties of groups : Cancellation Laws,

(1) $ab = ac \Rightarrow b = c$, $ba = ca \Rightarrow b = c$.

(2) $ax = b \Rightarrow x = a^{-1}b$, $ya = b \Rightarrow y = ba^{-1}$.

(3) $(ab)^{-1} = b^{-1}\ a^{-1}$ and $(a^{-1})^{-1} = a$.

4. Permutation : A one-one onto mapping of a finite set onto itself is called permutation and when this permutation replaces n objects cyclically it is called cyclic permutation.

5. Transformation. A cycle of the form (a, b) which interchanges only the elements a and b and rest of the elements remain unchanged is called a transposition.

6. Addition, multiplication modulo m:

$a+b$ (mod. m) or $(a+b)$ (mod. $m)=r$

where r is the least non negative remainder when $a+b$ or $a\times b$ is divided by m.

7. Residue classes modulo m : An integer a is said to be congruent to another integer b modulo m if $a-b$ is divisible by m *i.e.* $a-b=km$.

8. Order of an element a of a group is n if n is the least+ive integer such that $a^n=e$.

The order of any power of an element of a group cannot exceed the order of a. Also the order of a and a^{-1} are same.

9. One-one mapping : The mapping $f: G\to G'$ is said to be one-one if

$f(x)=f(y) \Rightarrow x=y$ or $x\neq y \Rightarrow f(x)\neq f(y)$

In other words different elements of G have different f images in G'.

10. Isomorphism of groups : Let $f: G\to G'$ such that f is one-one and onto mapping preserving group compositions in G and G' *i.e.* $f(a\ o\ b)=f(a)\ o'\ f(b)$ then G is isomorphic to G' *i.e.* $G\simeq G'$.

11. Properties of isomorphic mapping : Identities and inverses correspond.

i.e. $f(e)$ is identity of G' where e is identity of G

$f(a^{-1})=[f(a)]^{-1}$ *i.e.* image of the inverse of an element is the inverse of the image of that element.

12. Cayley's Theorem : Every finite group is isomorphic to a permutation group.

13. Cyclic group : A group capable of being generated by a single element a is called a cyclic group.

14 Sub group : A non empty sub set H of group G is said to be a sub group of G if

(1) H is stable in G *i.e.* composition in G induces composition in H *i e.* $a\,b \in H \;\forall\; a, b \in H$.

(2) H satisfies all the postulates of a group for the induced composition.

15. Criteria for a sub group :

$$a \in H, b \in H \Rightarrow a\,b^{-1} \in H.$$

For finite groups.

$$a \in H \;\; b \in H \Rightarrow a\,b \in H.$$

16. Cosets : $H=\{h_1, h_2, ..,h_n\}$ is a sub group of a group G and a is any element of G then the set

$\{h_1\,a, h_2\,a, ..., h_m\,a\}$ denoted by $H\,a$ is called right coset and the set $\{a\,h_1, a\,h_2, ..., a\,h_m\}$ denoted by $a\,H$ is called left cosets.

i.e. $H\,a=\{h\,a : h \in H\}$, $a\,H=\{a\,h : h \in H\}$

17. Properties. 1. $hH=Hh=H \;\;\forall\;\; h \in H$. *i.e.* right and left cosets corresponding to any element $h \in H$ are H.

2. Any two right (left) cosets of a sub group are either disjoint or identical

3. $H\,a=H\,b \Rightarrow a\,b^{-1} \in H$ where $a, b \in G$

$a\,H=b\,H \Leftrightarrow b^{-1}\,a \in H$ where $a, b \in G$.

18. Lagranges Theorem : The order of a sub group H of a finite group G is a divisor of the order of the group G.

Rings

1. Ring. Definition : A non empty set R with two binary compositions denoted as '+and .' is called a ring $(R, +, .)$ if

R_1 The set R is an abelian group for addition composition.

R_2 Multiplication composition is associative *i.e.*

$$(a.b).c=a.(b.c).$$

R_3 Multiplication is both right and left distributive with regard to addition.

i.e. $a.(b+c)=a.b+a.c$

and $(b+c).a=b.a+c.a.$

The additive identity is called zero of the ring and the multiplicative identity denoted by 1 is called unity of the ring.

2. Types of rings :

(a) Commutative ring *i.e* $a\,b=b\,a\ \forall\ a, b \in R.$

(b) Ring with Unity *i.e.* $a.1=1.a\ \forall\ a \in R.$

(c) Ring with zero divisors : If the product of two non zero elements of R is zero *i.e*.

$$a\,b=0 \Rightarrow a\neq 0,\ b\neq 0.$$

(d) Ring without zero divisors. If the product of no two non zero elements is zero *i.e.*

$a\,b=0 \Rightarrow a=0$ or $b=0$ or $a=0$ and $b=0.$

3. Integral domain : A ring $(R, +, .)$ with more than one element is called an integral domain if

(a) It is a commutative ring

(b) It is a ring with unity.

(c) It is a ring without zero divisors.

4. Field : A ring $(R, +, .)$ which has at least two elements is called a field if

(a) It is a commutative ring.

(b) It is a ring with unity

(c) All non zero elements are inversible.

Alternate definition : Combining the above properties we can say that a ring $(R, +, .)$ is called a field if its non-zero elements form an abelian group under multiplication.

5. Skew field (Division Ring) : A ring $(R, +, .)$ having at least two elements is called a skew field if it is a ring with unity and is such that every non zero element has a multiplicative inverse belonging to it.

It differs from the field in the sense that it is a non commutative ring.

6. Isomorphism of two rings. If their exists a one-one onto mapping $f : R \to R'$ such that

$f(a+b)=f(a)+f(b)$

$f(a\,b)=f(a)\ f(b)\ \forall\ a, b \in R$ then R is said to be isomorphic to R' *i.e.* $R \cong R'$.

7. Sub rings : $(R, +, .)$ is a ring and S is a sub set of R such that S is closed for both the compositions $+$ and $.$ then S is called a sub ring.

8. Sub field : A sub set S of a field $(F, +, .)$ is said to be a sub field of F if S is a field w.r.t addition and multiplication in F.

9. Left Ideal.

A non empty sub set S of $(R, +, .)$ is said to be a left ideal of R if

(i) S is a sub group of R w.r.t. addition

i.e. $\forall\ a, b \in S, a-b \in S$.

(ii) $r\,s \in S\ \forall\ r \in R$ and $\forall\ s \in S$ [r on the left]

In case $s\,r \in S\ \forall\ r \in R$ and $\forall\ s \in S$ [r on the right]

Then S is called **right ideal.**

Two sided ideal.

In case $r\,s \in S$, $s\,r \in S\ \forall\ r \in R$ and $\forall\ s \in S$ then S is both left and right ideal.

10. Principal ideal. An ideal generated by a single element a of the ring *i.e.* (a) is called a principal ideal.

11. Null and unit ideal The ideal generated by zero element and unit element are called null and unit ideal respectively.

12. Principal ideal ring. A ring for which every ideal is a principal ideal is called a prncial ideal ring.

Vector Spaces

1. Vector Space : $(F, +, .)$ is a field whose elements are termed as scalars and V be a non empty set whose elements are called vectors. There is an internal binary composition $+$ in V and an external composition in V over F called scalar multiplication satisfying the following axiom.

$\forall\ \alpha, \beta \in V$ and $a, b \in F$.

(1) $(V, +)$ is an abelian group.

(2) The multiplication of vectors by scalars satisfy the following

$$a(\alpha+\beta)=a\alpha+a\beta$$
$$(a+b)\alpha=a\alpha+b\alpha$$
$$(ab)\alpha=a(b\alpha) \text{ and } 1\alpha=\alpha.$$

Then the set V is called a vector space over the field F and is denoted as $V(F)$.

2. Properties of Vector space :

(1) $a.0=0$. (2) $0.\alpha=0$. (3) $(-a)\alpha=-(a\alpha)$

(4) $a(-\alpha)=-(a\alpha)$ (5) $a(\alpha-\beta)=a\alpha-a\beta$.

3. Vector sub space : A non empty sub set W of a vector space $V(F)$ is called a sub space of $V(F)$ if W is a vector space over F w.r.t. addition and scalar multiplication.

4. Criteria for a sub space :

$$\left.\begin{aligned}\alpha \in W, \beta \in W &\Rightarrow \alpha-\beta \in W\\ a \in F, \alpha \in W &\Rightarrow a\alpha \in W\end{aligned}\right\}$$

Alternate $\alpha, \beta \in V, a, b \in F \Rightarrow a\alpha+b\beta \in W$.

5. Linear sum of two sub spaces W_1 and W_2.

$W_1+W_2=\{\alpha_1+\alpha_2 : \alpha_1 \in W_1, \alpha_2 \in W_2\}$.

Direct sum of two sub spaces

$V=W_1 \oplus W_2$ *i.e.* V is the direct sum of two sub spaces W_1 and W_2 if

(a) $V=W_1+W_2$, (b) $W_1 \cap W_2=\{0\}$.

In other words if a vector $z \in V$ is uniqualy expressible as $z=\alpha_1+\alpha_2$ with $\alpha_1 \in W_1$ and $\alpha_2 \in W_2$.

6. Linear Dependence and Independence :

If $a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n=0$ where $a_i' \in F$ and $\alpha_i' \in V$.

If all the a' are not zero then the set of vectors $\{\alpha_1, \alpha_2,\ldots,\alpha_n\}$ is said to be linearly dependent. If however $\sum a_i\alpha_i=0 \Rightarrow a_i=0$ for each i. *i.e.* all the scalars are zero then the set is said to be linearly independent.

7. (a) A set containing at least one zero vector is L.D

(b) The singleton set $\{\alpha_1\}$ is L.I. iff $\alpha_1 \neq 0$.

(c) Any sub set of a L.I set is L.I.

(d) Any super set of L.D. set is L.D.

(e) The set of non zero vector $\{\alpha_1, \alpha_2,\ldots,\alpha_n\}$ of $V(F)$ is L.D. iff α_k can be expressed as a L C. of the vectors which preceede it. $2 < k \leqslant n$.

8. Linear Span of a set :

Linear span $L(S)$ of a non empty sub set S of a $V(F)$ is the set of all linear combinations of any finite number of element of S.

i.e. $L(S)=\{a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n : \alpha_i \in S, a_i \in F\}$.

9. $L(S)$ is a sub space of $V(F)$.

10. Bases :

The sub set S of $V(F)$ is called a basis if

(a) S is linearly independent set of vectors in V.

(b) $L(S)=V$ *i.e.* every vector in V is a linear combination of elements of S.

11. Finite dimensional or finitely generated vector spaces :

A vector space $V(F)$ is said to be finitely generated if there exists a finite sub set S of V such that $V=L(S)$.

12. There exists a basis for each finite dimensional vector space and any two basis of such a space have the same number of elements.

13. Every L. I. set of vectors of $V(F)$ can be extended to form a basis set.

14. Linear Transformation :

$f: U(F) \to V(F)$ is said to be a linear transformation if

$$f(\alpha+\beta)=f(\alpha)+f(\beta) \quad \forall\ \alpha, \beta, \in U(F)$$

and $$f(a\alpha)=a\, f(\alpha) \quad \forall\ a \in F, \alpha \in U(F).$$

Combining the above two we can say that

$$f(a\alpha+b\beta)=af(\alpha)+bf(\beta).$$

15. Linear operator and functional :

$f: U \to U$ then f is a linear operator.

Linear functional

$f: U \to F$ then f is linear functional.

16. Vector space Isomorphism :

$f: U(F) \to V(F)$ such that

f is one-one, onto and

$f(a\alpha+b\beta)=a\,f(\alpha)+b\,f(\beta) \quad \forall\ a, b \in F, \alpha, \beta \in U(F)$

then f is called an isomorphism and the two vector spaces are said to be isomorphic *i.e.* $U(F) \cong V(F)$.

17. Two finite dimensional vector spaces are isomorphic if and only if their dimensions are equal.

18. Every n dimensional vector space $V(F)$ is isomorphic to $V_n(F)$

19. Dim $W \leqslant$ dim V where W is a sub space.

20. If $V=W_1 \oplus W_2$ then

$$\dim V=\dim W_1+\dim W_2.$$

21. $\dim(W_1+W_2)=\dim W_1+\dim W_2-\dim(W_1 \cap W_2)$

22. Quotient Space.

If W be any sub space of $V(F)$ then the set

$V/W=\{W+\alpha, \alpha \in V\}$ is a vector space over F for the two compositions defined as

$$(W+\alpha)+(W+\beta)=W+(\alpha+\beta) \quad \forall\ \alpha, \beta \in V$$

$$a(W+\alpha)=W+a\,\alpha, \alpha \in V, a \in F.$$

23. $\dim V/W=\dim V-\dim W.$

CHAPTER I

GROUPS

§ I. Binary composition (operation).

Definition : *If G be a non empty set and $a, b \in G$ then a composition denoted as o such that $a\ o\ b \in G$ is called a binary composition on the set G.*

In other words a binary composition in a set G is a mapping of $G \times G$ into G which associates to each ordered pair (a, b) of members of G, a member of G.

Illustration :

(a) Consider the set of integers I. The operation of addition $+$ and multiplication ' . ' and subtraction $-$ are all binary compositions because,

$$a\ o\ b = a + b = \text{integer} \in I$$
$$a\ o\ b = a\ .\ b = \text{integer} \in I$$
$$a\ o\ b = a - b = \text{integer} \in I.$$

But the operation of division $\div$ is not a binary composition because $a\ o\ b = a \div b$ which may or may not be an integer, *i.e.* $a\ o\ b$ may or may not belong to the set I.

Again if we restrict the set **I to be the set of +ive integers** only then the operation of subtraction $-$ is also not a binary operation because $a\ o\ b = a - b$ may be $+$ive integer or $-$ive integer and as such it may or may not belong to the set of $+$ive integers.

Similarly if we consider the set R of real numbers then argued as above $+ - \times$ are all binary operations but division is not a binary operation because $a\ o\ b = a \div b =$ real no doubt but $a \div 0$, *i.e.* $a/0$ is meaningless, *i.e.* for any two

elements a, 0 of R we do not get an element of R under the operation of division and as such it is not a binary operation.

If however we exclude the number zero and take our set as R_0 the set of non zero real numbers then the operation of division $\div$ is also a binary operation.

$\because$ $a \circ b = a \div b =$ real number $\in R_0$ whenever $a, b \in R_0$.

(b) Again let us conider a set of vectors in space then the operation of addition, subtraction and vector product of vectors are all binary operations as $\mathbf{a}+\mathbf{b}$, $\mathbf{a}-\mathbf{b}$ and $\mathbf{a}\times\mathbf{b}$ are all vectors and as such belong to the set of vectors On the other hand the operation of dot product of vectors is not a binary operation because $\mathbf{a} \cdot \mathbf{b}$ = scalar and not a vector and as such it does not belong to the set of vectors.

Again if we restrict the **set of vectors to only coplanar vectors**, then the operation of vector product will also not be a binary operation because $\mathbf{a} \circ \mathbf{b} = \mathbf{a}\times\mathbf{b}$ = vector perpendicular to the plane of **a** and **b** and as such it will not belong to the set of coplanar vectors to which **a** and **b** belong and hence it is not a binary operation.

(c) In the set of all $m \times n$ matrices the operation of addition and subtraction of matrices are binary operations because $\mathbf{A}+\mathbf{B}$ and $\mathbf{A}-\mathbf{B}$ are again $m \times n$ matrices as such belong to the set.

Similarly in the set of all $n \times n$ matrices the multiplication of matrices is a binary operation.

(d) Similarly in the power set of a given set the operation of union $\cup$ and intersection $\cap$ are both binary operations as we now that the union and intersection of two subsets of a given set are again sub-sets of the set.

(e) Again the L. C. M. or H. C. F. of two natural numbers is again a natural number and hence in the set of

natural numbers the operation of L. C. M. and H. C. F. are binary operations.

§ 2 Various Types of Compositions.

(a) Associative Compositions. In a set G the composition denoted as o is said to be **associative** if,

$$(\mathbf{a}\ o\ \mathbf{b})\ o\ \mathbf{c}=\mathbf{a}\ o\ (\mathbf{b}\ o\ \mathbf{c})\ \forall\ \mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbf{G}.$$

It should be clearly understood that the above must hold for all $a, b, c \in G$. If the above holds good for some particular members $a, b, c \in G$ but not for all then the composition will not be termed as associative. In this case the algebraic structure (G, o) where G is the set and o the composition is said to be associative.

Illustration.

(1) In the set of numbers the composition of addition and multiplication are both associative, whereas the subtraction is not an associative composition.

(2) In the set of all $m \times n$ matrices the addition composition is associative because

$$(A\ o\ B)\ o\ C=(A+B)+C$$

$$A\ o\ (B\ o\ C)=A+(B+C)$$

and we know that $(A+B)+C=A+(B+C)$, where A, B, C are matrices of $m \times n$ type.

(3) In the set of vectors in space the operation of vector product is not an associative operation because.

$$(\mathbf{a}\ o\ \mathbf{b})\ o\ \mathbf{c}=(\mathbf{a}\times\mathbf{b})\times\mathbf{c}=\mathbf{c}.\mathbf{a}\ \mathbf{b}-\mathbf{c}\ \mathbf{b}\ \mathbf{a}$$

whereas $\mathbf{a}\ o\ (\mathbf{b}\ o\ \mathbf{c})=\mathbf{a}\times(\mathbf{b}\times\mathbf{c})=\mathbf{a}\ \mathbf{c}\ \mathbf{b}-\mathbf{a}\ \mathbf{b}\ \mathbf{c}.$

$$\therefore\quad (\mathbf{a}\ o\ \mathbf{b})\ o\ \mathbf{c}\neq\mathbf{a}\ o\ (\mathbf{b}\ o\ \mathbf{c})$$

and hence not associative.

(4) In the set Q show that the composition defined as $a\ o\ b=a+b+ab$ is associative.

$$(a\ o\ b)\ o\ c=(a+b+ab)\ o\ c$$
$$=(a+b+ab)+c+(a+b+ab)\ c$$
$$=a+b+c+ab+bc+ac+abc.$$

Again $a\ o\ (b\ o\ c)=a\ o\ (b+c+bc)$
$$=a+(b+c+bc)+a\ (b+c+bc)$$
$$=a+b+c+ab+bc+ac+abc$$
$$=(a\ o\ b)\ o\ c.$$ Hence associative.

(b) **Composition with identity element.** In a set G the composition denoted as o is said to be composition with identity element denoted by e **if there exists an element e belonging to G such that**

$$a\ o\ e=a=e\ o\ a\ \forall\ a\in G.$$

This element $e\in G$ is called the identity element and the algebraic structure (G, o) is said to be having identity element.

Illustration. In the set of real, or rational numbers with additive composition the identity element is zero where as if the composition be multiplication, then identity element is 1, because $x+0=x=0+x$ and $x.1=x=1.x$, $\forall\ x\in$ above sets.

However, if we consider the set Q_0, *i.e.* the set of non zero rational numbers or the set of natural numbers or R_0, the set of non zero real numbers, then for additive composition it has no identity element because 0 could be the identity element but 0 does not belong to Q_0 or R_0 or N. **The identity element if it exists must belong to the set.**

In the set of $m\times n$ matrices for additive composition the null matrix of $m\times n$ type is the identity element whereas in the set of all $n\times n$ matrices with multiplicative composition the unit matrix of $n\times n$ type is the identity element.

Again in the power set $P(S)$ of a given set with composition as Union of sets $\cup$ the null set ϕ is the identity element whereas, for the composition of intersection of sets

$\cap$, the set S is the identity element. $\therefore\ \phi \cup A = A \cup \phi = A$ whereas $A \cap S = S \cap A = A$

(c) Invertible elements in a set equiped with a composit on and having an identity element. Let G be a set with a composition denoted by o and e be the identity element, then an element $a \in G$ is said to be invertible if there exists an element $b \in G$ such that $a\ o\ b = e = b\ o\ a$ and in that case b is said to be inverse of element a and is written as $b = a^{-1}$.

It should be noted that inverse of an element must belong to the set.

Illustration. In the set of integers, rational, real or complex numbers with additive composition every element is invertible, because 0 is the identity element and the inverse of any element x of the above sets is $-x$ because $x + (-x) = 0$, *i e.* identity $= (-x) + x$.

Again in the set of non zero rational, real or complex numbers with multiplicative composition every element is invertible because 1 is the identity element and the inverse of any element x of the above sets is $\frac{1}{x}$ because

$$x \cdot \frac{1}{x} = 1, \quad i.e.\ \text{identity} = \frac{1}{x} \cdot x$$

If however we consider the set of natural numbers with multiplicative composition and the identity element being 1 none of the element of the set except 1 is invertible because in this case inverse of $x \in N$ will be $\frac{1}{x}$ which is not an integer and as such does not belong to the set of natural numbers whereas the inverse of an element must also belong to the set.

Similarly in the set $(I, .)$, the only inversible elements are 1 and -1 and the rest are not invertible.

Again in the set of all squared non singular matrices with matrix multiplication as composition each element is invertible.

(d) Commutative Composition.

In the set G a composition denoted by o is said to be commutative if for all $a, b, \in G$

$$a \; o \; b = b \; o \; a$$

and in this case the algebraic structure (G, o) is said to be commutative or **abelian.**

Illustration. In the set of vectors with vector product as the composition, we can say that it is not commutative because

$$\mathbf{a \; o \; b = a \times b} \text{ and } \mathbf{b \; o \; a = b \times a = -(a \times b)}$$

i.e. $a \; o \; b \neq b \; o \; a$ and hence not commutative.

In the set of numbers the additive and multiplicative compositions are commutative whereas subtraction and division compositions are not commutative.

§ 3. Groups. (Meerut 1968, Lucknow 64, 67 Allahabad 65, Gorakhpur 65, Sagur 70, Delhi 70 Gujart 70, Kanpur 69, Agra 69)

Definition. *A non empty set G with a binary composition denoted by o and satisfying the following properties is called a group.*

G_1 **The composition is associative.**

i.e. $(a \; o \; b) \; o \; c = a \; o \; (b \; o \; c) \; \forall \; a, b, c \in G.$

G_2. **Existence of identity.**

$\forall \; a \in G$ there exists an **unique** (to be proved later on) element $e \in G$ such that

$$a \; o \; e = e \; o \; a = a.$$

G_3. **Existence of inverse.**

$\forall \; a \in G$ there exists an element $b \in G$ such that

$a \; o \; b = b \; o \; a = e$ (the identity element).

The element b is called inverse of a and is denoted by a^{-1} so that we can say that

$$a^{-1} \; o \; a = a \; o \; a^{-1} = e.$$

Abelian Group.

If in addition to the above three properties the binary composition in G **is commutative**

i.e. $a \circ b = b \circ a \ \forall \ a, b \in G$ then the group G is called **abelian or commutative.**

Some definitions.

(a) *A* set G with *a* binary composition is said to be a **groupoid.**

(b) *A* set G with a binary composition which is associative is said to be **semigroup.**

(c) *A* set G with a binary composition which is associative and identity element exists is said to be a **monoid.**

Particular Cases

We have chosen to denote the binary composition by the symbol 'o'. We could however use the symbol * as well or to be more specefic the symbol + or . according as the binary composition in G is that of addition or multiplication. The properties G_1, G_2, G_3 will in these cases be read as under.

$\forall \ a, b, c \in G.$

G_1 $(a \circ b) \circ c = a \circ (b \circ c)$

$(a+b)+c = a+(b+c)$ for + composition

$(a.b).c = a.\ (b.c)$ for . composition

G_2 $(a \circ e) = (e \circ a) = a$

$a+0 = 0+a = a$ for + composition

$a.1 = 1.a = a$ for . composition

G_3 $(a \circ b) = (b \circ a) = e.$

$a+(-a) = (-a)+a = 0$ the identity for + composition

$a.\frac{1}{a} = \frac{1}{a}.a = 1$ the identity for . composition

or $a\,a^{-1} = a^{-1}\,a = 1$

For Abelian.

$(a \circ b) = (b \circ a)$

$a+b \cdot b+a$ for $+$composition

$a\ b = b.a$ for .composition

Note. In some books the the properties (2) and (3) stated above are given as under,

Existence of identity *i.e.* $e \circ a = a\ \forall\ a \in G$,

In this case e is called left identity and we shall later on show that $e \circ a = a \Rightarrow a \circ e = a$ *i.e.* the existence of right identity.

Existence of inverse *i e.* $a^{-1} \circ a = e\ \forall\ a \in G$,

In this case a^{-1} is called left inverse and we shall show later on that $a^{-1} \circ a = e \Rightarrow a \circ a^{-1} = e$, *i.e.* the existence of right inverse.

Finite and Infinite Groups. (Luck. 68, Gorakhpur 70)

If the number of elements in the set G forming a group be finite then it is called a finite group and the number of elements in it is called the order of this finite group. Otherwise it is called an infinite group and it is said to be of infinite order or zero order.

EXERCISE 1

Groups of Numbers

Ex. 1. *The set I of all integers, i. e.*

$$\{ \ldots -4, -3, -2, -1, 0, 1, 2, 3, 4 \ldots\ldots \}$$

is a group with respect to the operation of addition.

(Lucknow 67; Allahabad 64; Gorakhpur 65; Meerut 70)

In order to prove that the above set for the given operation is a group we have to satisfy all the three properties of the group and also that the operation is binary, *i.e.*

$$a \circ b = a+b \in I\ \forall\ a, b \in I$$

which is true as the sum of any two integers is again an integer.

This is sometimes referred as **the closure property for the group and** it is implied when we say that the operation is binary.

Associative. $\forall\ a, b, c \in I$, we have

$$(a+b)+c=a+(b+c)$$

because the associative law holds for integers.

Identity. The number $0 \in I$, is the identity element because $\forall\ a \in I$ we have $a+0=a=0+a$.

Inverse. For all element $a \in I$, $\exists -a \in I$ such that $(-a)+a=0$ (identity)$=a+(-a)$.

Abelian. Again $\forall\ a, b \in I$, we have $a+b=b+a$ and hence the composition is commutative.

Hence the given set is an abelian group for the operation of addition and we shall refer this group as the **additive group of integers** and denote it by $(I, +)$. Again since the set I contains infinite number of elements and as such the group $(I, +)$ is an abelian group of inifinte order.

Particular Cases.

We have proved above that the set $(I, +)$ is a group Below we shall consider some subsets of I and find whether they are groups are not and give reasans.

1. $G=\{-3, -2, -1, 0, 1, 2, 3\}$, *for* $+$

It is not a group because closure property is not satisfied *as* $2+3=5$ but $5 \notin G$.

2. $N=\{$*The set of natural numbers*$\}$, *for* $+$

It is not a group because there does not exist any identity element **in the set** (note). Yes you may say that $5+0=0+5=5$ and hence 0 is identity element; but zero does not belong to the set. G_3 says that identity element should exist and **belong to the set.**

3. $E=\{$*The set of all even Integers*$\}$, *for* $+$

(Lucknow 67; Gorakhpur 65)

Yes it is a group. (Note that $0=2\times 0$ and as such 0 is an even integer).

4. $o=\{$*The set of all odd integers*$\}$, *for* $+$ **(Allahabad 64)**

It is not a group as closure property is not satisfied because sum of two odd integers is an even integer and as such does not belong to the set. In other words the composition of addition is not a binary composition.

5. $I=\{$*The set of all iutegers*$\}$ *for.* (*multipiication*).

It is not a group because G_3 *i.e.* inverse property is not satisfeed you may say that $5 \cdot \frac{1}{5}=\frac{1}{5} \cdot 5=1$ (the identity)

$\therefore$ inverese of 5 is $\frac{1}{5}$ but $\frac{1}{5}$ is not an integer and as such does not belong to the set.

6. $I=\{$*The set of all integer*$\}$, *for*$=$(*subtraction*)

It is not a group, because the property G_1 *i.e.* associative is not satisfied $\because$ $a\ o\ (b\ o\ c)=a-(b-c)=a-b+a$

$(a\ o\ b)\ o\ c=(a-b)-c=a-b-c$

$\therefore$ $(a\ o\ b)\ o\ c\neq a\ o\ (b\ o\ c)$

7. $Q_0=\{$*The set of non-zero rational numbers*$\}$, *for* (*multiplication*), $+$

Yes, it will be a group for multiplication. In this case as compared to case 5 the inverse will exist and belong to the set. For addition it will not be a group because the identity element, thoughzero shall not belong to set

8. $Q=\{$*The set of all rational numbers including zero*$\}$ *for* (*multiplication*)

If will not be a group as the inverse of element zero in Q will not exist.

9. $G=\{$*The set of multiples of all integers by a fixed integer m*$\}$, *for*$+$

i.e. $G=\{\ldots\ldots -3m, -2m, -m, 0, m, 2m, 3m, \ldots\}$ for $+$,

Let $a, b \in G \quad \therefore \quad a=rm,\ b=sm$ where $r, s \in I$

1. $a+b=rm+sm=(r+s)m=km : \quad k \in I$
2. Associative or addition in the set of integers is always associative.
3. zero is the identity.
4. $a+(-a)=rm+(-r)\ m=(r-r)\ m=0\cdot m=0$
   $(-a)+a=(-r)m+rm=(-r+r)\ m=0\cdot m=0$

$\therefore$ Inverse exists and belongs to the set. Hence $(G, +)$ is a group.

Q. 2 *Prove that the set*

$G=\{\ldots\ldots 2^{-4}, 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3, 2^4 \ldots\ldots\}$

forms an infinte abelian group. w.r.t, multiplication.

Let $a, b \in G \Rightarrow a=2^r,\ b=2^s$ where r and s are some integers.

$\therefore \quad a\,b=2^{r+s}=2^k$ where $k=r+s$ is also an integer and hence $a\,b \in G$ whenever a and $b \in G$ so that multiplication is a binary composition.

Multiplication of rational numbers is always associative.

The identity element is clearly 1 and $\in G$ and inverse of any element $a=2^r$ is 2^{-r} which also belongs to G such that

$$2^r \cdot 2^{-r} = 2^{-r} \cdot 2^r = 1, \text{ the identity.}$$

The inverse of element 1 is 1 itself

Again since the multiplication of rational numbers is commutative and because the set G consists of infinite number of elements therefore G is an infinite abelian group.

Ex. 3. *Prove that the set C of all complex numbers*

$$Z=a+ib,\ a, b \in R$$

forms an infinite abelian group w. r. t. addition of complex numbers.

We know that sum of two complex numbers is again a complex number so that addition in set C is a binary composition.

Also it is well known that addition of complex numbers is associative. Clearly the complex number $0+i0$ which belongs to C is the identity element and the inverse of any element $Z=a+ib$ is $-Z=-a-ib$, which is the additive inverse of Z and it belongs to the set.

Again $(a+ib)+(c+id)=(a+c)+i\,(b+d)$

$=(c+a)+i\,(d+b)=(c+id)+(a+ib)$.

$\because$ $a+c=c+a$ and $b+d=d+b$

as addition in R is commutative.

Hence the addition in the set C is commutative.

Therefore the $(C,+)$ is an abelian groups and since it contains infinite number of elements and hence it is an infinite abelian group.

Ex. 4. *Prove that the set C_0 of all non zero complex numbers is a group w. r. t multiplication of complex numbers.*

$C_0=\{Z : Z=a+ib$ where $a,\ b \in R$ and both a and b are not zero$\}$

Let $\alpha=a+ib$, $\beta=c+id$ be two numbers of C_0 then

$\alpha.\beta=(a+ib)\,(c+id)=(ac-bd)+i\,(bc+ad)$

which is again a complex number and is not a zero complex number because if it is a zero complex number $0+0i$ then it would mean that $ac-bd=0$ and $bc+ad=0$. But these will hold good only if either both $a=0, b=0$ or both $c=0, d=0$ which is not possible as α and $\beta \in C_0$ are non zero complex numbers. Thus $\alpha\beta$ also $\in C_0$ and as such multiplication is a binary composition.

Further we know that multiplication of complex numbers is always associative. Again the complex numbers $1+0i$

i e. 1 is the identity element. Also inverse of any non zero complex number $a+ib$ is

$$\frac{1}{a+ib}=\frac{a-ib}{(a+ib)\ (a-ib)}=\frac{a-ib}{a^2+b^2}$$

$$=\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2} \text{ where } a^2+b^2\neq 0 \text{ because } a \text{ and } b \text{ both are not zero}$$

$$=x+iy \quad \text{where } x, y \in R \text{ and are not both zero.}$$

Hence the inverse of every element exists and belongs to set C_0.

Thus $(C_0, .)$ is a group and because multiplication of complex numbers is commutative therefore the group is an abelian group.

Ex. 5. *Prove that the set of all complex numbers z such that $|z|=1$ forms a group with respect to multiplication of complex numbers.*

Let $z=a+ib$. $\therefore$ $|z|=\sqrt{(a^2+b^2)}=1$ or $a^2+b^2=1$ which in turn means that both a and b cannot be zero.

Also $|z_1 z_2|=|z_1||z_2|=1$

and hence multiplication is a binary composition which is associative. Identity is $1+0i$ and its mod is also 1 and inverse of $a+ib$ as shown in last example is

$$\frac{a}{a^2+b^2}+i\frac{-b}{a^2+b^2}, \text{whose mod is}$$

$$\frac{a^2}{(a^2+b^2)^2}+\frac{(-b)^2}{(a^2+b^2)^2}=\frac{1}{a^2+b^2}=1$$

as $a^2+b^2=1$ given. Thus inverse exists and belongs to the set.

Hence the given set forms a group for multiplication.

Ex. 6. *Prove that the following sets form a group under ordinary multiplication as composition.*

(i) $G=\{a+b\sqrt{2} : a, b \in Q\}$

(ii) $G=\{a+ib : a, b \in Q\}$.

where both a and b are not zero.

Let $\alpha=a+b\sqrt{2}$ and $\beta=c+d\sqrt{2}$ be any two elements of the set then $\alpha.\beta=(ac+2bd)+(ad+bc)\sqrt{2}$ and it is of the form $x+y\sqrt{2}$ $(x, y \in Q)$ and hence closure property is satisfied. Associative property follows from the usual rule of associativity of numbers

Identity is $1+0\sqrt{2}$ *i.e.* 1.

Inverse of $a+b\sqrt{2}$ is $\dfrac{1}{a+b\sqrt{2}}=\dfrac{a-b\sqrt{2}}{a^2-2b^2}$

$$=\frac{a}{a^2-2b^2}+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \text{ and } \in G.$$

$$=x+y\sqrt{2} \text{ where } x, y \in Q$$

Hence the inverse exists and belongs to set G, therefore $(G,.)$ is a group

Note. If $a, b \in I$, then in this case it will not form a group because $\dfrac{a}{a^2-2b^2}$ will not be an integer and as such the inverse of an element shall not belong to the set.

(ii) Similarly we can prove the second part.

Ex. 7. *Prove that the sets of Ex.* 6 *constitute a group under ordinary addition as the composition.*

Ex. 8. *The set* $A=\{1, \omega, \omega^2\}$, *where* $1, \omega, \omega^2$ *are cube roots of unity and* $\omega^3=1$ *forms a group w.r.t. multiplication composition.* **(Luck 70; Agra 70; Gorakhpur 66)**

Multiplication is a binary operation, because the product of any two elements of A is again an element of A. Clearly associative property is satisfied as the product of complex numbers obey the associative law. Identity element is 1 because the row headed by 1 coincides with top row thereby emphasizing that $1\cdot 1=1$, $1.\omega=\omega$, $1.\omega^2=\omega^2$ and inverse of each element exists and belongs to the set *e.g.* $1^{-1}=1$,

$$\omega^{-1}=\frac{1}{\omega}=\frac{\omega^2}{\omega^3}=\omega^2,\ (\omega^2)^{-1}=\frac{1}{\omega^2}=\frac{\omega}{\omega^3}=\omega,$$

The above can be exhibited in a tabular form as under.

In order to find the inverse of any element say ω^2 you have to look to the row in which leading element is ω^2 *i.e.* 3rd row. See the identity element 1 in that row. The element in the head of that column *i.e.* 2nd column which is ω will be its inverse, $\therefore$ Inverse of $\omega^2=\omega$. Similarly inverse of ω is ω^2 etc.

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	$\omega^3=1$
ω^2	ω^2	$\omega^3=1$	$\omega^4=\omega$

Ex. 9. ***Prove that the set consisting of the four fourth roots of unity forms an abelian group w.r. t. multiplication compisition.*** **(Luck. 66)**

Let $x=1^{1/4}$ $\therefore$ $x^4-1=0$ or $(x^2+1)(x^2-1)=0$

$\therefore$ $x=1, -1, i, -i.$

Let us form the composition table for multilpicat on.

Multiplication

i.e.	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	$+i$
i	i	$-i$	1	1
$-i$	$-i$	i	1	-1

From the above table it is clear that multiplication is a binary operation as all the elements inside the above table are elements of G. Again multiplication of complex numbers is always associative. Also we observe that the row headed by 1 coincides with the top row thereby emphasizing that $1.1=1$, $1\cdot(-1)=-1$, $1\ (i)=i$, $1\ (-i)=-i$ and as such 1 is the identity element. We can verify that the inverse of each element exists and belongs to the set, For example we check up the inverse of $-i$.

Look to the row in which leading element is -1 *i.e.* 4th row. See the identity element 1 in that row then the number at the head of this column *i.e.* i wiil be inverse of $-i$. Thus $(-i)^{-1}=i$.

Similarly $(1)^{-1}=1$, $(i)^{-1}=-i$,

Again we know that multiplication of complex numbers is always commutative and hence the above set is an abelian group for multiplication.

Rule to judge the commutative property from the table.

In case you find from the table that the elements in each row are the same as the elements in each of the corresponding column in the table then we say that the composition is commutative e.g. you may see that R_4 is same as C_4 and similarly all other rows and columns are identical.

Note. After going through the above examples the students may be inclined to feel that we can have groups only of numbers and that too under the compostion of addition and multiplication. Here below we shall give some more examples of groups in which not only the elements are not numbers but the compositions are also not ordinary addition and multiplication.

Ex. 10. *Prave that the set of all vectors in space do not form a group with respect to vector multiplication as composition, but is a group w.r.t. vector addition.*

Vector multiplication is a binary operation as $\mathbf{a}\times\mathbf{b}$ is again a vector but the composition is not associative because, $(\mathbf{a}\times\mathbf{b})\times\mathbf{c}\neq\mathbf{a}\times(\mathbf{b}\times\mathbf{c})$. [See P. 3].

Vector addition is associative The zero vector $\mathbf{o}$ is the identity and inverse of any vector $\mathbf{a}$ is $-\mathbf{a}$. Also sum of two vectors is again *a* vector. Hence a group. Again since $\mathbf{a}+\mathbf{b}=\mathbf{b}+\mathbf{a}$ *i.e.* commutative therefore abelian group.

Note. *The set of all ve tors do not form a group for dot product as the composition.*

$\mathbf{a}.\mathbf{b}=a\,b\cos\theta$ *i.e.* scalar and not a vector.

Hence closure property is not satisfied.

Ex. 11. *Prove that the set of all $m\times n$ matrices having their elements as integers (rational, real or complex numbers) is an infinite abelian group with matrix addition as composition.* **(Lucknow 67)**

Sum of any two $m\times n$ matrices is again a $m\times n$ matrix and hence matrix addition is a binary operation. Also we know that matrix addition is associative. The null matrix is the identity element. The inverse of any matrix A is $-A$. Again since $A+B=B+A$ *i.e.* matrix addition is commutative and hence the given set forms an infinite abelian group

Ex. 12. *Prove that the set of all $n\times n$ non singular matrices having their elements as rational (real or complex) numbers is an infinite non abelian group with matrix multiplication as composition. If the elements were integers then will it be a group ?*

(Lucknow 67 ; Meerut M. Sc. 1967 B. Sc. 71)

The product of two $n\times n$ non singular matrices is again a $n\times n$ non singular matrix and hence matrix multiplication

is a binary operation. Again we know that matrix multiplication is associative when all the matrices are $n \times n$ type. Clearly unit matrix I_n is the identity element. Also we know that every non singular matrix is inversible and if A is non singular then A^{-1} is also non singular. Hence the inverse of each matrix exists and belongs to the set.

Also since $AB \neq BA$ in general so the composition is not commutative. Hence a non-abelian group.

In case the elements of the matrices were restricted to be integers only then it will not form a group because in that case the inverse of any matrix may have elements which are not integers and as such it shall not belong to the set *e.g.* we may verify that if $A = \begin{bmatrix} 1 & 2 \\ 3 & 2 \end{bmatrix}$ then $A^{-1} = \begin{bmatrix} -\frac{1}{2} & \frac{1}{2} \\ \frac{3}{4} & -\frac{1}{4} \end{bmatrix}$

Now A^{-1} does not belong to the set as its elements are not integers.

Ex. 13. *Prove that the set of matrices*

$$A_\alpha = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix}$$

where α *is real (integral or rational) form a commutative group relative to matrix multiplication.* **(Kanpur 69 ; Alld. 66)**

$G = \{A_\alpha : \alpha \in R \text{ or } I \text{ or } Q\}$

Let $A_\alpha, A_\beta \in G$ then

$$A_\alpha . A_\beta = \begin{bmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{bmatrix} \begin{bmatrix} \cos\beta & -\sin\beta \\ \sin\beta & \cos\beta \end{bmatrix}$$

$$= \begin{bmatrix} \cos(\alpha+\beta) & -\sin(\alpha+\beta) \\ \sin(\alpha+\beta) & \cos(\alpha+\beta) \end{bmatrix}$$

$$= A_{\alpha+\beta} \in G$$

as whenever $\alpha, \beta \in R$ or I or Q then $\alpha+\beta \in R$ or I or Q. Hence closure property is satisfied.

Again we know that matrix multiplication is associative when all the matrices are $n \times n$ type.

The unit matrix $I=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ or $\begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix}$

$=A_0$ is the identify element

$$\in G \text{ as } 0 \in R,\ I \text{ or } Q$$

Also

Inverse. Again since $|A_\alpha| = \cos^2\alpha+\sin^2\alpha=1\neq 0$, therefore A_α is non-singular and hence inverse exists.

Also $A_\alpha^{-1}=\dfrac{\text{adj. } A_\alpha}{|A_\alpha|}$

$$=\begin{bmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{bmatrix}=\begin{bmatrix} \cos(-\alpha) & -\sin(-\alpha) \\ \sin(-\alpha) & \cos(-\alpha) \end{bmatrix}$$

$\therefore$ $A\alpha^{-1}=A_{(-\alpha)}$ and it clearly belongs to G.

Again $A_\alpha . A_\beta = A_{\alpha+\beta}=A_{\beta+\alpha}=A_\beta . A_\alpha$. Hence commutative property is also satisfied as

$$\alpha+\beta=\beta+\alpha \ \forall\ \alpha, \beta \in R,\ I \text{ or } Q.$$

Ex. 14. *Prove that the set* $G=\{(\cos\theta+i\sin\theta) : \theta$ *runs over all rational numbers}* *forms an infinite abelian group with respect to ordinary multiplication.*

$A_\alpha . A_\beta=(\cos\alpha+i\sin\alpha)(\cos\beta+i\sin\beta)$

$=\cos(\alpha+\beta)+i\sin(\alpha+\beta)$

$\therefore$ $A_\alpha . A_\beta = A_{\alpha+\beta}$ etc.

$A_0=\cos 0+i\sin 0=1=$identity.

Again $(\cos\alpha+i\sin\alpha)(\cos\alpha-i\sin\alpha)=\cos^2\alpha+\sin^2\alpha=1$

$\therefore$ $A_\alpha^{-1}=\cos\alpha-i\sin\alpha$

$=\cos(-\alpha)+i\sin(-\alpha)=A_{-\alpha}$.

Again since $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$ it follows that

$(A_\alpha . A_\beta) . A_\gamma = A_\alpha . (A_\beta . A_\gamma)$ *i.e.* associative.

Also as $\alpha+\beta=\beta+\alpha$

$\therefore$ $A_\alpha A_\beta = A_\beta A_\alpha$ *i.e.* commutative.

Hence an infinite abelian group.

Ex. 15. (a) *Prove that the set Q of all rational numbers other than 1 with the operation defined by $a \circ b = a+b-ab$ constitutes an abelian group.* **(Kanpur M. Sc. 69)**

Let $a, b \in Q$ so that both a and b are rational numbers other than 1.

$\therefore$ $a \circ b = a+b-a\,b$ is also a rational number other than 1 because if it is equal to 1

i.e. if $a+b-a\,b=1$ then $a+b-a\,b-1=0$ or $(a-1)(1-b)=0$.

This would mean that

$a=1$ or $b=1$ which is not true. Hence $a \circ b \in Q$ *i.e.* the operation $\circ$ is a binary operation.

Associative. $(a \circ b) \circ c = (a+b-a\,b) \circ c$

$$= (a+b-a\,b)+c-(a+b-a\,b)\,c$$
$$= a+b+c-a\,b-a\,c-b\,c+a\,b\,c.$$

Also $a \circ (b \circ c) = a \circ (b+c-b\,c)$

$$= a+(b+c-b\,c)-a\,(b+c-b\,c)$$
$$= a+b+c-a\,b-a\,c-b\,c+a\,b\,c.$$

Thus $(a \circ b) \circ c = a \circ (b \circ c)$ and hence associative,

Identity. If e be the identity then

$$a \circ e = a, \Rightarrow a+e-a\,e=a.$$
$$\Rightarrow e\,(1-a)=0 \Rightarrow e=0 \text{ as } a \neq 1$$

and in this case

$$a \circ e = a \circ 0 = a+0-a\,0=a.$$

Hence 0 is the identity.

Inverse $a \circ b = a+b-a\,b$ 0 the identity

$\Rightarrow \dfrac{a}{a-1} = b$ is the inverse of a.

Also since $a-1 \neq 0$.

$\therefore$ $\dfrac{a}{a-1}$ is a rational number other than 1 and as such belongs to Q. Therefore inverse exists and belongs to the set.

Commutative $a \circ b = a+b-a\,b = b+a-b\,a = b \circ a$,
Hence commutative,
Therefore an abelian group.

Note. In a similiar manner prove that the set Q of all rational numbers other then -1 with the operation defined by $a \circ b = a+b+a\,b$ constitutes an abelian group,

Identity $=0$, Inverse of a is $-\frac{a}{a+1}$ etc.

In a similar manner we can prove the following.

Ex, 15 (b). Q_{-1}=*{set of all rational numbers other than* -1*} is an abelian group for the composition defined as*

$$a \circ b = a+b+a\,b$$

Identity is zero, $a^{-1}=\frac{a}{a+1}$ $(a \neq -1)$.

Ex. 15 (c). I=*{Set of all integers} for the composition defined as* $a \circ b = a+b+1$ *is also an abelian group*

Identity is -1, $a^{-1}=-a-2$

Ex. 16. *Prove that the set* Q^+ *of all positive rational numbers forms an abelian group for the composition* o *defined as* $a \circ b = \frac{a\,b}{2}$ **(Delhi Hon's 70)**

Let $a, b \in Q^+$

$\therefore$ $a \circ b = \frac{a\,b}{2} \in Q^+$ Hence closure property.

Associative. $(a \circ b) \circ c = \frac{a\,b}{2} \circ c = \frac{\left(\frac{a\,b}{2}\right) c}{2} = \frac{a\,b\,c}{4}$

$$a \circ (b \circ c) = a \circ \frac{b\,c}{2} = \frac{a\left(\frac{b\,c}{2}\right)}{2} = \frac{a\,b\,c}{4}$$

Hence $a \circ (b \circ c) = (a \circ b) \circ c$

Identity. If e is the identity then

$$a \circ e=a \Rightarrow \frac{a e}{2}=a$$

$$\Rightarrow a(e-2)=0$$

$$\Rightarrow e=2 \text{ as } a \neq 0 \text{ as } a \in Q^+$$

Also $2 \in Q^+$

$\therefore$ Identity exists and belongs to the set.

Inverse, Let b be the inverse of a

$$\therefore \quad a \circ b=e \Rightarrow \frac{a b}{2}=2 \Rightarrow b=\frac{4}{a}$$

and as $a \in Q^+ \quad \therefore \quad b=\frac{4}{a} \in Q^+$

$\therefore$ Inverse exists and belongs to the set.

Commutative. $a \circ b=\frac{a b}{2}=\frac{b a}{2}=b \circ a \quad \forall\ a, b \in Q^+$.

Hence Q^+ is a commutative group.

Ex 17. *A set G consists of ordered pairs (a, b) such that a, b are real and $a \neq 0$. A binary composition $\circ$ is defined in G as under.*

$$(a, b) \circ (c, d)=(a c, b c+d).$$

Prove that the given set constitutes a group for the given composition. **(Raj. M Sc 69,66)**

The composition is given to be binary.

Associative. $\{(a, b) \circ (c, d)\} \circ (e, f)$

$$=(a c, b c+d) \circ (e, f)=((a c) e, (b c+d) e+f)$$

$$=(a c e, b c e+d e+f) \qquad \ldots(1)$$

$(a, b) \circ \{(c, d) \circ (e, f)\}$

$$=(a, b) \circ \{c e, d c+f\}=(a (c e), b (c e)+de+f)$$

$$=(a c e, b c e+d e+f) \qquad \ldots(2)$$

From 1 and 2 we find the composition $\circ$ is associative.

Identity. Let (p, q) be the identity element so that

$(a, b) \circ (p, q)=(a, b) \Rightarrow (a p, b p+q)=(a, b)$

$\Rightarrow a\,p=a$ and $b\,p+q=b \Rightarrow p=1$ and $q=0$

So that (1, 0) is the identity element which belongs to the set.

Inverse. Let (x, y) be the inverse of an element (a, b) of G then

$$(a, b)\ o\ (x, y)=\text{Identity}=(1, 0)$$

$\Rightarrow (a\,x, b\,x+y)=(1, 0) \Rightarrow a\,x=1,\ b\,x+y=0$

$\Rightarrow x=1/a$ and hence $y=-b/a$.

$$(a, b)^{-1}=(x, y)=(1/a, -b/a).$$

Now because $a\neq 0$ as given therefore inverse exists and belongs to the set.

Hence the set S is a group for the given composition.

Since $(a, b)\ o\ (c, d)=(a\,c, b\,c+d)$

But $(c, d)\ o\ (a, b)=(c\,a, d\,a+b)$.

$\therefore$ $(a, b)\ o\ (c, d)\neq(c, d)\ o\ (a, b)$ *i.e.* the composition is not commutative and hence the group is not abelian.

Note. In case o be defined as

$(a, b)\ o\ (c, d)=(a\,c, b\,d)$ than also it will be a group

and $e=(1, 1)$ and $[(a, b)]^{-1}=\left(\frac{1}{a}, \frac{1}{b}\right)$ etc etc.

Ex. 18. *S is a non void set and A and B are sub sets of S which belong to the power set $P(S)$. An operation o is defined on the elements of $P(S)$ as*

$$A\ o\ B=A \cup B$$

Verify whether $P(S)$ will be a group or not.

(Raj. M. Sc. 66)

Union of sets is always associative

i. e. $(A \cup B) \cup C=A \cup (B \cup C)$.

Again $A \cup \phi=A=\phi \cup A$ and hence the empty set ϕ is the identity element.

Let A be a non empty set of $P(S)$ and if its inverse be say X then $A\ o\ X=A \cup X\neq\phi$ the identity.

Hence the inverse of non empty member of $P(S)$ will not exist.

Therefore $P(S)$ is not a group for the given composition.

Ex. 19. *Prove that the set of all n, nth roots of unity form a finite abelian group G under multiplication as composition.* **(Gorakhpur 67, Banares 65, 69, Allahabad 64, 67, 70)**

We know that $u=(1)^{1/n}=(\cos\theta+i\sin\theta)^{1/n}$.

$$=(\cos 2r\pi+i\sin 2r\pi)^{1/n}$$

or $$u=\cos\frac{2r\pi}{n}+i\sin\frac{2r\pi}{n}=e^{i(2\pi r)/n}$$

where $r=0, 1, 2, 3,\ldots\ldots,n-1$.

Hence n, nth roots of unity are

$$G=\{1, e^{2\pi i/n}, e^{4\pi i/n},\ldots,e^{2(n-1)\pi i/n}\}$$

Let us choose $a=e^{\frac{2\pi r_1}{n}i}$ and $b=e^{\frac{2\pi r_2}{n}i}$

any two elements of the set where $0\leqslant r_1\leqslant n-1$

and $$0\leqslant r_2\leqslant n-1$$

$$ab=e^{\frac{2\pi(r_1+r_2)}{n}i}$$

and it will belong to the set if $r_1+r_2\leqslant n-1$.

But if $r_1+r_2>n-1$, then let $r_1+r_2=n+q$ where $q\leqslant n-2$, because the max. value of r_1+r_2 can be $n-1+n-1=2n-2$ and hence $q\leqslant n-2$,

$\therefore$ In this case $ab=e^{\frac{2\pi(r_1+r_2)}{n}i}=e^{\frac{2\pi(n+q)}{n}i}$

$$=e^{2\pi i}e^{\frac{2\pi q}{n}i}$$

But $e^{2\pi i}=\cos 2\pi+i\sin 2\pi=1$.

$\therefore$ $ab=e^{\frac{2\pi q}{n}i}$ where $q\leqslant n-2$.

Hence $ab\in G$ in either case thus showing that multiplication is a binary operation or the closure property is satisfied.

Again since multiplication of complex numbers is associative and as such the given composition is associative.

Also the identity element is 1 *i.e.* $e^{\frac{2\pi.0}{n}i}$.

Inverse of any element $a=e^{\frac{2\pi r_1}{n}i}$ is $e^{\frac{2\pi(n-r_1)}{n}i}$

because $e^{\frac{2\pi r_1}{n}i}.e^{\frac{2\pi(n-r_1)}{n}i}=e^{2\pi i}=1=$ Identity.

We also know that multiplication of complex numbers is commutative and hence the set G is a finite abelian group w.r.t. multiplication.

Ex. 20. *The adjoining table defines a certain binary operation o on the set $A=\{a, b, c, d, e\}$. Show that the set A forms a group w.r.t. the binary operation o and find the inverse of each element.*

How to read the table.

For any two elements c and e of A the operation $c\ o\ e$ gives the element at the intersection of row headed by c and column headed by e, *i.e.* the element b within brackets in the table.

o	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	(b)
d	d	e	a	b	c
e	e	a	(b)	c	d

Similarly $e \circ c=b$ within bracket, $b \circ d=e$ and $d \circ b=e$. Thus the operation $\circ$ on any two elements of the set gives another element of the set and so it is a binary operation.

Associative $(a \circ b) \circ c=(b \circ c) \quad \because \quad (a \circ b)=b.$

$=d. \quad \because \quad (b \circ c)=d.$

Again $a \circ (b \circ c)=a \circ d=d.$

$\therefore \quad (a \circ b) \circ c=a \circ (b \circ c).$

Identity : From the table $a \circ a=a$, $b \circ a=a \circ b=b$. $c \circ a=a \circ c=c$, $d \circ a=a \circ d=d$, $e \circ a=a \circ e=e$,

Hence a is the identity element.

Inverse : The inverse of any element $d \in A$ will be x such that $d \circ x=x \circ d=a$ the identity.

We should look for the identity element a in the row headed by d, and the element at the top of that column will be x.

i.e. $d \circ c=a$. Also $c \circ d=a$. $\therefore$ inverse of d is c.

Similarly inverse of c is d.

Again inverse of e is $b \quad \because \quad e \circ b=a$ and $b \circ e=a$ and inverse of b is e.

Inverse of a is a.

Hence a group.

Ex. 21. *Prove that the four matrices*

$$A=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ B=\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix},\ C=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ D=\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$$

form a multiplicative group. Is it abelian or not.

Here A is a unit matrix so that $AA=A$, $AB=BA=B$, $AC=CA=C$, $AD=DA=D$.

Also $BC=\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}=D=CB$,

$$BD=\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}=C=DB \text{ etc.}$$

Hence we have the following composition table.

From above table as verified by actual multiplication we find that the product of any two matrices is again a matrix of the set and so closure property is satisfied.

×	*A*	*B*	*C*	*D*
A	*A*	*B*	*C*	*D*
B	*B*	*A*	*D*	*C*
C	*C*	*D*	*A*	*B*
D	*D*	*C*	*B*	*A*

e.g. $C \times D = B$ *i.e.* matrix at the intersection of row headed by C and column headed by D.

Also $D \times C = B$.

Also associative $\therefore \quad (A \times B \times C = B \times C = D$

$\because \quad A \times B = B$

$$A \times (B \times C) = A \times D = D.$$

$$\therefore \quad (A \times B) \times C = A \times (B \times C).$$

Identity. The matrix A is the identity because the row headed by A coincides with the top row.

Inverse. From the table the inverse of matrices A, B, C, D are A, B, C, D respectively which belong to the set *e.g.* In order to find inverse of C, look to the row headed by C *i.e.* third row and see the identity element A in this row then the matrix at the top of the column will be the inverse of C which is C from the table.

Since each row is identical with the corresponding column, therefore the composition is commutative. Hence an abelian group.

Ex. 22. *Prove that the set of four transformations* f_1, f_2, f_3, f_4 *on the set of complex numbers defined by*

$$f_1(z)=z,\ f_2(z)=-z,\ f_3(z)=1/z,\ f_4(z)=-1/z$$

forms a finite abelian group w. r. t. the composition known as composite of two functions or product of two functions.

(Benares M. Sc. 63)

We know that if $f : U \to V$ and $g : V \to W$.

Then the composite transformation

$$(g\ o\ f) : U \to W$$

defined as $$(g\ o\ f)\ x=g[f(x)]\ \forall\ x \in U \in V.$$

In this case $(f\ o\ g)$ will not be defined. However if U, V and W coincide that is to say when f and g are operators then both $g\ o\ f$ and $f\ o\ g$ or $g\ f$ and $f\ g$ are defined.

Also we know that $f\ I=f=I\ f$,

where I is the identity operator. In the present case f_1, f_2, f_3, f_4 are all operators and as such all possible products are defined. Since $f_1(z)=z$ therefore f_1 is an identity operator.

Products w. r. t. f_1. Where f_1 is the identity operator.

$$f_1\ o\ f_1=f_1,\ f_1\ o\ f_2=f_2\ o\ f_1=f_2,\ f_1\ o\ f_3=f_3\ o\ f_1=f_3,$$
$$f_1\ o\ f_4=f_4\ o\ f_1=f_4.$$

Products w. r. t. f_2.

$$f_2\ o\ f_1=f_1,\ (f_2\ o\ f_2)\ z=f_2(f_2(z))=f_2(-z) \text{ by definition}$$
$$=-(-z)=z=f_1(z)$$
$$\therefore\ f_2\ o\ f_2=f_1.$$
$$(f_2\ o\ f_3)\ z=f_2[f_3(z)]=f_2(1/z)=-1/z=f_4(z).$$
$$\therefore\ f_2\ o\ f_3=f_4=f_3\ o\ f_2$$
$$(f_2\ o\ f_4)\ z=f_2[f_4(z)]=f_2(-1/z)=1/z=f_3(z).$$
$$\therefore\ f_2\ o\ f_4=f_3=f_4\ o\ f_2$$

Products w. r. t. f_3.

$f_3\ o\ f_1=f_3,\ f_3\ o\ f_2=f_2\ o\ f_3=f_4$ as shown above.

$$f_3\ o\ f_3\ (z)=f_3[f_3(z)]=f_3(1/z)=1/(1/z)=z=f_1(z)$$
$$\therefore\ f_3\ o\ f_3=f_1$$

$$f_3 \, o \, f_4 \, (z) = f_3 \, [f_4 \, (z)] = f_3 \, (-1/z) = 1/-(1/z) = -z = f_2 \, (z)$$

$$\therefore \quad f_3 \, o \, f_4 = f_2 = f_4 \, o \, f_3.$$

Product w. r. t. f_4.

$f_4 \, o \, f_1 = f_1$, $f_4 \, o \, f_2 = f_2 \, o \, f_4 = f_3$, $f_4 \, o \, f_3 = f_3 \, o \, f_4 = f_2$

as shown above

$$f_4 \, o \, f_4 \, (z) = f_4 \, [f_4 \, (z)] = f_4 \, [-1/z] = -1/-(1/z) = z = f_1 \, (z)$$

$$\therefore \quad f_4 \, o \, f_4 = f_1.$$

Thus we have formed all possible products of the given four functions.

Let us now form the composition table

o	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Since all the elements in the table are element of $\{f_1, f_2, f_3, f_4\}$ and as such the set is closed for multiplication Also products of operators is always associative.

The row headed by f_1 is same as the top row so that f_1 is the identity element. Inverse of each element exists and belongs to the set. For finding the inverse of say f_3 look to the row headed by f_3 *i.e.* 3rd row and look to the identity element f_1 in that row then element at the head of this column *i e.* f_3 will be the inverse of f_3 *i.e.* $f_3^{-1} = f_3$.

It can be verified because $f_3^{-1} \, o \, f_3 = f_3 \, o \, f_3 = f_1$ as shown above. Similarly we can show that

$$f_1^{-1} = f_1, \; f_2^{-1} = f_2, \; f_4^{-1} = f_4.$$

Since each how is identical with the corresponding column in the table and hence composition is commutative *i.e.* $f_i \circ f_j = f_j \circ f_i \ \forall\ i, j$.

Hence an abelian group which is finite.

Ex. 23. *Show that the set of six transformations* $f_1, f_2, \ldots, f_6$ *on the set of complex numbers defined by*

$$f_1(x)=x,\ f_2(x)=\frac{1}{x},\ f_3(x)=1-x,\ f_4(x)=\frac{x}{1-x},$$

$$f_5(x)=\frac{1}{1-x},\ f_6(x)=\frac{x-1}{x}$$

forms a finite non abelian group of order 6 w. r. t. composite operation.

Students have got to compose all possible products and we have the following composition table

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

As in part (a) the closure property is satisfied, also the composition is associative, f_1 is the identity.

Inverse of each exists and belongs to the set.

e.g. for inverse of f_5 look to the row headed by f_5 and see the identity element f_1 in that row then the element f_6 at the head of the column is inverse of f_5.

$\therefore\quad (f_5)^{-1}=f_6$ etc.

Hence a group.

Again since $f_3 \, o \, f_4 = f_5$ but $f_4 \, o \, f_3 = f_6$.

$\therefore \quad f_3 \, o \, f_4 \neq f_4 \, o \, f_3$

therefore the composition is not commutative.

We may also say that each row is not identical with corresponding column *e.g.* 3nd row is not same as 3rd column and hence the composition is not commutative.

Hence a finite non abelian group of order 6.

Ex. 24. *Verify whether the set G for the defined composition o is a group or not.*

$G = \{a_i : i \in N \text{ and } 0 \leqslant i < 7\}$

and $a_i \, o \, a_j = a_{i+j}$ *where* $i+j < 7\}$

$a_i \, o \, a_j = a_{i+j-7}$ *when* $i+j \geqslant 7$ **(Kanpur M. Sc. 1969)**

$G = \{a_0, a_1, a_2, a_3, a_4, a_5, a_6\}$

where $a_1 \, o \, a_3 = a_4 \quad \because \quad 1+3 < 7, a_2 \, o \, a_4 = a_6 \quad \because \quad 2+4 < 7$

But $a_3 \, o \, a_5 = a_{8-7} = a_1$

$\because \quad 3+5 \geqslant 7, a_2 \, o \, a_5 = a_{7-7} = a_0 \quad \because \quad 2+5 \geqslant 7$

Hence keeping in view the composition o as defined we have the following composition table

o	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_0	a_0	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6	a_0
a_2	a_2	a_3	a_4	a_5	a_6	a_0	a_1
a_3	a_3	a_4	a_5	a_6	a_0	a_1	a_2
a_4	a_4	a_5	a_6	a_0	a_1	a_2	a_3
a_5	a_5	a_6	a_0	a_1	a_2	a_3	a_4
a_6	a_6	a_0	a_1	a_2	a_3	a_4	a_5

Since all the elements inside the table are elements of G and hence closure property is satisfied. Again as the row headed by a_0 is the same as the top row therefore a_0 is the identity element. Since the identity element a_0 is present in each row therefore inverse of each element exists and it is found as explained in Ex. 23, 22.

Elements.	a_0	a_1	a_2	a_3	a_4	a_5	a_6
Inverses.	a_0	a_6	a_5	a_4	a_3	a_2	a_1

i.e. $a_i^{-1}=a_{7-i}$

Again each row is identical with corresponding column and hence the composition is commutative.

i.e. $a_i \circ a_j=a_j \circ a_i \ \forall\ i, j : 0 \leqslant i, j < 7$

Associative. We know that $(i+j)+k-i+(j+k)$ when $i, j, k \in N$.

$\therefore \quad (a_i \circ a_j) \circ a_k=a_i \circ (a_j \circ a_k)$

and each is equal to a_l where $l=i+j+k < 7$

or each is equal to a_{l-7} where $l=i+j+k \geqslant 7$

Hence the given set constitutes a finite abelian group.

§ 4. Addition and multiplication modulo m.

If a and b be two integers then by addition modulo m expressed as $a \underset{m}{+} b$ we mean the least non-negative number r which is the remainber when $a+b$ is divided by m. In other words after adding a and b we remove the integral multiples of m and the remainder r which will be a +ve number less than m will be equal to $a \underset{m}{+} b$. $\therefore \ a \underset{m}{+} b=r$ where $0 \leqslant r < m$.

i.e.

$$3 \underset{6}{+} 20=23=6\ (3)+5=5$$

$$7 \underset{6}{+} 5\ =12=6\ (2)+0=0$$

$$-20 \underset{6}{+} 5=-15=6\ (-3)+3=3.$$

Similarly $16=6\ (2)+4=4$.

We say $16\equiv 4 \pmod 6$

i.e. 16 is congruent to 4 modulo 6.

$$-28=6\ (-5)+2=2$$

i.e. $$-28\equiv 2 \pmod 6.$$

Multiplication Modulo m.

If a and b be two integers then by multiplication modulo m expressed as $a \underset{m}{\times} b$ we mean the least non-negative number a which is the remainder when ab the ordinary product of a and b is divided by m. In other words after multiplying a and b we remove the integral multiples of m from it and the remainder r which will be +ive number less than m will be equal $a \underset{m}{\times} b$. $\therefore a \underset{m}{\times} b = r$ where $0 \leq r < m$.

e.g. $$3 \underset{7}{\times} 20 = 60 = 7\ (8)+4=4$$

$$-4 \underset{5}{\times} 11 = -44 = 5\ (-9)+1=1.$$

Ex. 25. *Prove that the set* $G=\{0, 1, 2, 3, 4, 5\}$ *is a finite abelian group under ordinary addition reduced modulo 6 as the composition.*

Here we shall make the following composition table.

+6	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	(0) 4 *o* 2	1	2	3
5	5	0	1	(2) 5 *o* 3	3	4

$$5 \circ 3 = 5 +_6 3 = 8 =_6 (1) + 2 = 2.$$

This element is written at the intersection of the row headed by 5 and the column headed by 3. Similarly $4 \circ 2 = 4 + 2 = 6 =_6 (1) + 0 = 0$ and it is written at the intersection of the row headed by 4 and the column headed by 2 Both these are written within brackets in the table.

Binary Composition. From the above table we conclude that $a +_m b$ *i.e.* sum of any two elements of the set under addition modulo 6 belongs to the set as all the elements in the table are the elements of the set G. So the composition of addition modulo 6 is a binary composition *i.e.* closure property is satisfied.

Associative. The composition is associative because $(a+b)+c$ and $a+(b+c)$ both will have the same +ive remainder as when $a+b+c$ is divided by 6.

Identity. Clearly the element 0 of the set is the identity element for the composition.

Inverse. In order to find the inverse of any element say 4, look to the row headed by 4 and see where the identity element i.e. 0 is placed (circled in the table) then the element at the head of this column *i.e.* 2 will be the inverse of 4 Similarly the inverse of 0 is 0, inverse of 1 is 5, inverse of 2 is 4, inverse of 3 is 3 and inverse of 5 is 1. In other words the inverse of any element a is obtained by subtracting that element from 6.

Again from the table we find that $5 +_6 3 = 3 +_6 5 = 2$.

Hence the composition is commutative. Therefore it is an abelian group.

Ex. 26. *Is the set* $\{1, 2, 3, 4, 5\}$ *a group under addition modulo 6.*

Here we have omitted the element 0 and preparing the composition table as in last example, we have

$+_6$	1	2	3	4	5
1	2	3	4	5	0
2	3	4	5	0	1
3	4	5	0	1	2
4	5	0	1	2	3
5	0	1	2	3	4

The above operation is not a binary operation because $5 +_6 1 = 6 = 0$ and 0 does not belong to the set.

Again it has no identity element and hence it is not a group.

Theorem I. Additive group fo integers modulo m

In general. *The set* I_m *of* m *integers* $\{0, 1, 2, 3 \ldots m-1\}$ *is a group under the addition modulo* m *composition.*

The sum of any two elements will again be an element of the set under the given composition. 0 is the identity and the inverse of any element r will be $m-r$ because $r +_m (m-r) = m = 0$ (identity),

Also $$(a +_m b) +_m c = a +_m (b +_m c)$$

as each will leave the same +ive remainder when $a+b+c$ is divided by m.

Again since $a \underset{m}{+} b = b \underset{m}{+} a \ \forall\ a, b \in$ set,

hence the composition is commutative and as such a finite abelian group.

Note, If we omit zero from the above set then it will not be a group as the composition will not be binary.

$\because \quad 2 \underset{m}{+} m \underset{m}{-} 2 = m = 0, \ 3 \underset{m}{+} m \underset{m}{-} 3 = m = 0$

and 0 does not belongs to the set

Ex. 27. *Prove that the set {1, 2, 3, 4} of four integers is a finite abelian group under multiplication modulo 5.*

(Note 5 is prime)

The composition table is as shown below

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	(3)	2	(1)
		$4 \circ 2$		$4 \circ 4$

$$4 \circ 2 = 4 \underset{5}{\times} 2 = \underset{5}{8} \quad 5\,(1) + 3 = 3.$$

It is the element written at the intersection of the row headed by 4 and the column headed by 2. Similarly $4 \circ 4 = 4 \underset{5}{\times} 4 = \underset{5}{16} = 5\,(3) + 1 = 1.$

Both these are within brackets in the table.

Binary composition. From above table we conclude that $\forall\ a, b \in$ set $a \underset{5}{\times} b$ is again a member of the set and hence the composition is binary.

Associativity. $(a\ o\ b)\ o\ c$ and $a\ o\ (b\ o\ c)$ will give the same remainder as when the ordinary products $a\ b\ c$ is divided by 5.

Identity. Clearly the identity element is 1.

Inverse. In order to find the inverse of any element say 4 look to the row headed by 4 and come to the identiy element in that row then the element at the head of this column, *i.e*, 4 is the inverse of 4.

$\because$ $4.4 = \underset{5}{15} = 3\ (5)+1 = 1 =$ identity. Similarly inverse of 3 is 2 and that of 2 is 3 and of 1 is 1. Thus the inverse of each element exists and belongs to the set.

Again since $a.\underset{5}{b} = \underset{5}{b.a}\ \forall\ a, b \in$ set and as such the composition is commutative. Hence an abelian group.

Similarly we can prove that $G=\{1, 2, 3, 4, 5, 6\}$ is a finite abelian group under multiplication modulo 7. **(Agra 70)**

Ex. 28. *Is the set $\{1, 2, 3, 4, 5\}$ of five integers a group under the composition of multiplication modulo 6.*

(Note 6 is composite)

The composition table is as shown below.

$\times 6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The composition is not binary composition because $4.3=12=0$ under multiplication modulo 6 and 0 is not a member of the set. Also the inverse of each element does not exist, *e.g.* there is no inverse of the element 2 of the set.

Multiplicative group of integers modulo m, m prime.

Theorem 2. *In general set* $\{1, 2, 3, 4, \ldots, m-1\}$ *of* $m-1$ *integers will be a group under multiplication modulo m only when m is prime. In case m is composite then it will not be a group.* **(Meerut B. Sc. 1969)**

Multiplication modulo p is a binary operation.

Let $a, b \in G \quad \therefore \quad 1 \leqslant a \leqslant m-1, 1 \leqslant b \leqslant m-1.$

Now $a \underset{m}{\times} b = r$ where r is the least+ive remainder when $a\ b$ is divided by m. We shall show that $r \neq 0$ and that r lies between 1 and $m-1$ so that $a \underset{m}{\times} b = r$ also belongs to the set G.

Now neither a nor b are divisible by m as both are less than or equal to $m-1$. Also their product ab is also not divisible by m, because that would mean that m can be factorized but m is given to be prime. Hence $a \underset{m}{\times} b \neq 0$.

$$\therefore \quad a \underset{m}{\times} b = r \qquad \text{where} \qquad 1 \leqslant r \leqslant m-1.$$

Hence $a \underset{m}{\times} b$ belongs to the set G. Thus multiplication modulo m (m being prime) is a binary operation.

Associative. $(a \underset{m}{\times} b) \underset{m}{\times} c = a \underset{m}{\times} (b \underset{m}{\times} c)$ as each will leave the same remainder as when the ordinary product $a\ b$ is divided by m

Identity. Clearly the element $1 \in G$ is the identity element as $1 \underset{m}{\times} a = a = a \underset{m}{\times} 1$.

Inverse. Now we have to esablish that inverse of each element exists and is **unique.**

Let s be any element of G so that

$$1 \leqslant s \leqslant m-1.$$

Consider the following products

$$1 \underset{m}{\times} s,\ 2 \underset{m}{\times} s,\ 3 \underset{m}{\times} s, \ldots\ldots, (m-1) \underset{m}{\times} s.$$

Each of the above $m-1$ products are again elements of the set because of the binary composition. For existence we have to prove that one of these must be the identity element *i.e.* 1. For this we shall show that all the above $m-1$ products are distinct so that we get distinct $m-1$ elements of the set and only one of these will be the identity element 1 and as such we will automatically establish the uniqueness of inverse also.

Let i and j be both less than $m-1$ then consider the products.

$i \underset{m}{\times} s$ and $j \underset{m}{\times} s$. If they are not distinct then

$$i \underset{m}{\times} s = j \underset{m}{\times} s \Rightarrow i s - j s \text{ is divisible by } m.$$

$$\Rightarrow (i-j)\, s \text{ Is divisible by } m.$$

But m is prime therefore either $i-j$ is divisible by m or s is divisible by m, but $1 \leqslant s \leqslant m-1$ and each of i and j is also less than $m-1$ and as such $i-j$ is also not divisible by m, which is a contradiction. $\therefore$ $i \underset{m}{\times} s \neq j \underset{m}{\times} s$

Hence all the $m-1$ products

$$1 \underset{m}{\times} s,\ 2 \underset{m}{\times} s, \ldots\ldots, (m-1) \underset{m}{\times} s$$

are all distinct $m-1$ members of the set G and **only one** of them say $s' \times s = 1$ the identity of G.

Hence s' (only one) is the inverse of the element s of G.

Commutative. Since $a \underset{m}{\times} b = b \underset{m}{\times} a$ as each will leave the same least +ive remainder as when $a\,b$ is divided by m. The composition is commutative

$\therefore$ The set $\{G, \times_m\}$ is a finite abelian group of order $m-1$, m being prime.

2nd Case. When m is not prime then in this case m will be composite and let $m = a\,b$, where $a, b \in G$.

Now $a \underset{m}{.} b = m = 0$, under multiplication modulo m.

But 0 is not an element of the set and hence the above composition is n ot binary or the set is not closed w. r. t. the given composition and hence does not constitute a group.

Hence we conclude the following (Remember).

For additiou modulo m (m being any integer).

It will form a group if the set G contains first m integers including zero. If zero is excluded then it will not be a group.

$G = \{0, 1, 2, 3, 4, 5\}$ will be a group, for addition modulo 6.

But $G' = \{1, 2, 3, 4, 5\}$ will not be a group for addition modulo 6.

For multiplication modulo m.

It will form a group if the set G contains first $m-1$ non zero integers and if m is prime. If m is not prime it will not form a group.

$\therefore$ $G = \{1, 2, 3, 4\}$ under multiplication modulo 5 (prime) will be a group but

$G' = \{1, 2, 3, 4, 5\}$ under multiplication modulo 6 (6 not prime) will not be a group.

Ex. 29. *Prove that the following sets are groups.*

(a) $G=(0, 3, 6, 9)$ *for addition modulo 12.*

(b) $G=(1, 5, 7, 11)$ *for multiplication modulo 12.*

$+_{12}$	0	3	6	9
0	0	3	6	9
3	3	6	3	0
6	6	9	0	3
9	9	0	3	6

$9+9=18=6$ for $+_{12}$

$\cdot_{12}$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$7\times 11=77=5$ for $\cdot_{12}$

It is easy to verify as before that all the properties for being groups are satisfied.

§ 5. Residue classes modulo m.

Congruent modulo m :

An integer a is said to be congruent to another integer b modulo m (m being any fixed non zero integer) if $a-b$ is divisible by m.

i.e., $a-b=km$. where k is any integer and we express it as

$$a\equiv b \text{ (modulo } m)$$

We have already shown in set theory that the relation of congruent modulo m in the set **I** of all integers is an equivalence relation.

Residue classes modulo m :

Let I be a set of all integers and a relation R be defined congruent modulo 4.

or $x-y$ is divisible by 4 $\forall\ x, y \in I$. Above ralation is an equivalence relation.

Now $0 \in I$ and by equivalence class I_0 or [0] we shall mean the set of all those integers which are congruent to 0 mod. 4. *i.e.* if x be such as an integer then $x-0=4k$ for all $k \in I$. Give k values 0, 1, 2, 3, ...-1, -2, -3...we get

$$x=[...-12, -8, -4, 0, 4, 8, 12...]$$

or I_0 or $[0]=[...-12, -8, -4, 0, 4, 8, 12...]$

Similarly the residue class I_1 or [1] we shall mean the set of all those integers which are congruent to 1 modulo. 4. *i. e.*, $x-1=4k \ \forall \ k \in I$

$\therefore \quad x=[\,..-11, -7, -3, 1, 5, 9, 11...]=I_1=[1]$.

Similarly $I_2=[2]=[...-14, -10, -6, -2, 2, 6, 10\ ]$ from $x-2=4k$.

and $I_3=[3]=[...-9, -5, -1, 3, 7, 11..\ ]$

Again if we put $x-4=4k \ \forall \ k \in I$ we get $x=4\,(k+1)$. or $x-0=4n. \ \forall n \in I$. Above shows that the equivalence class I_1 is the same as I_0. Similarly $I_5=I_1$; $I_6=I_0$, $I_{15}=I_3$ etc.

The above equivalence classes have the following properties :

1. No two of them have any element common *i.e.*, they are mutually disjoint or $I_1 \cap I_2=\phi$.

2. The set I is the union of all the above equivalence classes.

3. All the integers in the same class have the relation of congruent modulo 4.

4. Integers in different classes do not have the relation of congruent modulo 4.

Sum and product of residue classes mod. m :

If $S\ \{\{0\}, \{1\}, \{2\},.....,\{r_1\}, ...,\{r_2\}, ...,\{m-1\}\}$

$\{r_1\}+\{r_2\}=\{r_1+r_2\}=\{r\}$ where r is the least +ive remainder when r_1+r_2 is divided by m.

Similarly $\{r_1\}.\ \{r_2\}=\{r_1\ r_2\}=\{r\}$ where r is the least +ive remainder when $r_1\ r_2$ is divided by m.

Theorem 3. *The residue classes modulo m form a finite group w. r. t. addition of residue classes.*

(Meerut B. Sc. 68; Allahabad 69; Benares M. Sc. 66)

Proof. Let S be the set of residue classes mod. m

i.e., $S=[\{0\}, \{1\},\ldots\ldots,\{r_1\}\ldots\ldots,\{r_2\},\ldots,\{m-1\}]$.

Closure. The sum of two residue classes $\{r_1\}$ and $\{r_2\}$ is $\{r_1\}+\{r_2\}=\{r_1+r_2\}=\{r\}$ where r is the least +ive remainder when $\{r_1+r_2\}$ is divided by m *i.e.*, $0 \leqslant r < m$. Hence $\{r\} \in S$. Thus the closure property is satisfied or addition of residue classes is a binary operation.

Associative, $[\{r_1\}+\{r_2\}]+\{r_3\}=\{r_1\}+[\{r_2\}+\{r_3\}]$
$=\{r_1\}+\{r_2\}+\{r_3\}$

because each will leave the same remainder as when $r_1+r_2+r_3$ is divided by m.

Identity, The identity element is $\{0\}$.

$\because$ $\{0\}+\{r\}=\{r+0\}=\{r\}$.

and $\{r\}+\{0\{=\{r+0\}=\{r\}$.

Inverse. Additive inverse of any element $\{r\}$ is $\{m-r\}$ because $\{r\}+\{m-r\}=\{m\}=\{0\}=$identity.

Again since the addition of residue classes is commutative and the number of elements are finite therefore the set S constitutes a finite abelian group w.r.t. addition of residue classes.

Theorem 4. *The non-zero residue classes modulo m* **where m is a composite integer** *do not form a group w. r. t. multiplication of residue classes.*

Since m is composite let $m=rs$ where $0 < r < m$, $0 < s < m$.

Now $\{r\}\{s\}=\{rs\}=\{0\}$ and $\{0\}$ does not belong to the set as the set consists of non-zero residue classes.

Therefore the closure property is not satisfied and hence the given set does not constitute a group under given composition.

Theorem 5. *The non-zero residue classes-modulo m where m is a positive prime integer form a group w. r. t. multiplication of residue classes.*

(Gorakhpur 70; Meerut B. Sc. 69)

Let $S=[\{1\}, \{2\}, ..,\{r_1\}, ..,\{r_2\},...,\{m-1\}]$.

Closure. $\{r_1\}.\{r_2\}=\{r_1r_2\}=\{r\}$ where r is the least +ive remainder when r_1r_2 is divided by m so that $0 < r < m$ and as such $\{r\} \in S$. $\therefore$ $\{r_1\}.\{r_2\} \in S$. Hence multiplication of residue classes is a binary operation.

Associative : $[\{r_1\}.\{r_2\}].\{r_3\}=\{r_1\}.[\{r_2\}.\{r_3\}]$ $=\{r_1\}.\{r_2\}.\{r_3\}$, as each will leave the same remainder as when $r_1r_2r_3$ is divided by m.

Identity : The identity element is clearly $\{1\}$, because $\{1\}.\{r\}=\{r\}.\{1\}=\{r\}$.

Inverse : The inverse of any element $\{r_1\}$ is $\{r_2\}$ where $r_1r_2 \equiv 1$ (mod. m). It should be clearly understood here that r_2 exists since the equation $r_1x=1$ (mod. m) has a solution.

Hence all the axioms of a group are satisfied and as such the given set S constitutes a group with respect to multiplication of residue classes.

Ex. 30. *Show that the residue class* $\{1\}, \{3\}, \{5\}, \{7\}$ *modulo 8 forms a multiplicative group.*

(Kanpur M. Sc. 1970)

We know $\{r_1\}\{r_2\}=\{r\}$ where r is the least +ive remainder when $r_1 r_2$ is divided by 8. Hence we have the following compositon table.

×	{1}	{3}	{5}	{7}
{1}	{1}	{3}	{5}	{7}
{3}	{3}	{1}	{7}	{5}
{5}	{5}	{7}	{1}	{3}
{7}	{7}	{5}	{3}	{1}

Since all the elements in the table are elements of the set therefore closure property is satisfied. Associative is as explained in Th. 6 Residue clase {1} is the identity element since {1} is present in each row therefore inverse of each element exists, and from the tatle we have.

elements	{1}	{3}	{5}	{7}
inverse	{1}	{3}	{5}	{7}

i.e. each element is its own inverse.

Again each row is identical with the corresponding column and hence multiplication is commuatative. Hence a finite abelian group.

§ 6. General properties of groups.

Let G be a group and o be the binary operation ; then $a\ o\ b$ will be written as ab using multiplicative notation. The identity will be denoted by e and the inverse of a will be denoted by a^{-1}. However if we use additive notation $+$ for o then e will be replaced by 0 (zero) and a^{-1} by $-a$.

Property 1. Left cancellation law.

If a, b. c $\in$ G then ab = ac $\Rightarrow$ b = c.

(Allahabad 70; Kanpur 69)

$ab=ac$ (given), $a^{-1} \in G$ and $ab, ac \in G$.

Operating on the left with a^{-1}, we get

$$a^{-1}(ab)=a^{-1}(ac)$$
$$\Rightarrow (a^{-1}a)\,b=(a^{-1}a)\,c \qquad \text{[Associative } G_1\text{]}$$
$$\Rightarrow \quad eb=ec \qquad \text{[Inverse } G_3\text{]}$$
$$\Rightarrow \quad b=c \qquad \text{[Identiy } G_2\text{]}$$

Hence proved

Property 2. The left identity element e is also the right identity element. **(Meerut 68)**

i.e. $ea=a \ \forall\ a \in G \Rightarrow ae=a \ \forall\ a \in G$

Let a^{-1} be the left inverse of a *i.e.* $a^{-1}a=e$ ...(1)

Now $a^{-1}(ae)=(a^{-1}a)\,e$ by associative property

or $a^{-1}(ae)=ee=e$ by I

or $a^{-1}(ae)=a^{-1}a$ by I

$\therefore$ $ae=a$ by Peoperty (1) *i.e.* L. C. Law.

$\therefore$ e is also the right identity.

So in future we shall call e the identity element and not the left identity or right identity.

Property 3. The left inverse of an element is also its right iaverse.

Let a^{-1} be the left inverse of a.

we have to prove that $a^{-1}a=e \Rightarrow a\,a^{-1}=e$

Now $a^{-1}(a\,a^{-1})=(a^{-1}a)\,a^{-1}$ by associative prop.

$=e\,a^{-1}$ $\because$ $a^{-1}a=e$ given

$=a^{-1}\,e$ [Left Identity = Right Identity]

$\therefore$ $a^{-1}(aa^{-1})=a^{-1}\,e$ hence $a\,a^{-1}=e$,

$\therefore$ a^{-1} is also right inverse of a.

Property 4. Right Cancellation Law. **(Allahabad 70)**

$$ba=ca \Rightarrow b=c \ \forall\ a, b, c \in G$$

$ba=ca$ $\therefore$ $(ba)\,a^{-1}=(ca)\,a^{-1}$

or $b\,(a\,a^{-1})=c\,(a\,a^{-1})$ by G_3

or $be=ce$

by right inverse Property 3

or $b=c$

by right identity Property 2.

Hence $ba=ca \Rightarrow b=c$.

Property 5. The equations ax=b and ya=b have unique solutions in G where a, b ∈ G (Allahabad 64)

$a \in G \therefore a^{-1} \in G$. Also $b \in G \therefore a^{-1} b \in G$.

Now $ax=b$. Put $a^{-1} b$ for x in this

$\therefore a\,(a^{-1} b)=b \Rightarrow (a\,a^{-1})\,b=b$ $[G_1]$

$\Rightarrow eb=b$ by $G_3 \Rightarrow b=b$ by G_2.

Hence $x=a^{-1} b$ is a solution of $ax=b$.

To show that the solution is unique.

If the solution be not unique then let x_1 and x_2 be two solutions of $ax=b$ so that $ax_1=b$ and $ax_2=b$.

$\therefore \quad ax_1=ax_2 \Rightarrow x_1=x_2$ by L. C. Law.

Hence the solution is unique.

Similarly $a \in G$. a^{-1}, G

Also $b \in G \quad \therefore \quad ba^{-1} \in G$.

Now $ya=b$. Put $y=ba^{-1}$.

$\therefore \quad (b\,a^{-1})\,a=b$ or $b\,(a^{-1}\,a)=b$ $[G_1]$

$\Rightarrow be=b$ by $G_3 \Rightarrow b=b$ by G_2.

Hence $y=ba^{-1}$ is a solution of $ya=b$.

Property 6. The identity element e in a group is unique. (Lucknow 67; Raj. 69; Allahabad 65)

Let if possible there be two identity elements e_1 and $e_2 \in G$.

Now e_1 is the identity $\therefore \quad e_1e_2 = e_2$. Left identity.

Again e_2 is the identity $\therefore \quad e_1e_2 \quad e_1$ Right identity.

From above relation it is clear that $e_1 = e_2$.

Alternative. We know that the equation $ax = b \ \forall \ a, b \in G$ has a unique solution $x = a^{-1} b$. Replacing b by a we get that $ax = a$ has a unique solution $a^{-1} a$ which is e and unique.

Similarly $ya = b$ has a unique solution $y = b\, a^{-1}$.

Replacing b by a we get $ya = a$ has a unique solution $y = a\, a^{-1}$ which is e and unique.

Property 7. The inverse of an element in a group is unique. **(Lucknow 67; Raj. 67; Allahabad 65; Meerut 68)**

Let a be an element of the group having two inverses b and c.

$$\therefore \quad ab = e = ba \quad \because \quad b \text{ is inverse of } a$$
$$ac = e = ca \quad \because \quad c \text{ is inverse of } a.$$

From above relation we get $ba = ca \Rightarrow b = c$ by R.C. law.

or $ab = ac \Rightarrow b = c$ by L. C. law.

Alternative. We know that the equation $ax = b \ \forall \ a, b \in G$ has a unique solution $x = a^{-1} b$. Replacing b by e we get that $ax = e$ has a unique solution $x = a^{-1} e = a^{-1}$ which is unique.

Similarly $ya = b$ has a unique solution $y = b\, a^{-1}$. Replacing b by e we get $ya = e$ has a unique solution $ea^{-1} = a^{-1}$ which is unique.

Property 8. The inverse of a is a^{-1}. To show that inverse of a^{-1} is a.

i.e. $$(a^{-1})^{-1} = a.$$

We know that $b^{-1} b = e \ \forall \ b \in G$.

Now if $a \in G$ then $a^{-1} \in G$. Replace b by a^{-1}

$$\therefore \quad (a^{-1})^{-1} a^{-1} = e$$

Operating on the right by a, we get

Operating on the right by a, we get

$[(a^{-1})^{-1}\, a^{-1}]\, a = ea \Rightarrow (a^{-1})^{-1}\, (a^{-1}\, a) = a$ by G_1, G_2

or $(a^{-1})^{-1}\, e = a$ or $(a^{-1})^{-1} = a$.

i.e. inverse of a^{-1} is a.

Alternative Metho .

We know that the solution of the equation $ax = b$ is $x = a^{-1}\, b$ which is unique.

Replacing a by a^{-1} and b by e, we get that the solution of $(a^{-1})\, x = e$ is $x = (a^{-1})^{-1}\, e = (a^{-1})^{-1}$. ...(1)

Again the solution of $(a^{-1}\, x) = e$ is obtained by operating by a on the left

$a\, (a^{-1}\, x) = ae$ or $(aa^{-1})\, x = a$ or $ex = a$ or $x = a$ ...(2)

Hence from (1) and (2), we get that $(a^{-1})^{-1}$ and a are solutions of the same equation $a^{-1}\, x = e$. But we know that the solution is unique and hence $(a^{-1})^{-1} = a$. Proved.

Property 9. Reversal Law.

To prove that the inverse of the product of two elements of a group is the product of their inverses in reverse order

i.e. $(ab)^{-1} = b^{-1}a^{-1}$.

(Meerut 68; Gorakhpur 68, Rajasthan 70)

Let $a, b \in G$ and a^{-1}, b^{-1} be their inverses in G.

So that $aa^{-1} = e = a^{-1}a$ and $bb^{-1} = e = b^{-1}b$ (1)

Now $(ab)\, (b^{-1}\, a^{-1}) = a\, [b\, (b^{-1}\, a^{-1})]$ by G_1

$= a\, [(bb^{-1}\ a^{-1}]$ by G_1

$= a\, [ea^{-1}]$ by (1)

$= aa^{-1} = e$ by (1).

Similarly we can show that $(b^{-1}\, a^{-1})\, (ab) = e$.

Hence $(ab)\, (b^{-1}\, a^{-1}) = e = (b^{-1}\, a^{-1})\, (ab)$.

Therefore the inverse of ab is $b^{-1}\, a^{-1}$, *i.e.* product of the inverses in reverse order.

Note. The above rule can be generalized as under

$$(abc..pq)^{-1}=q^{-1}p^{-1}...c^{-1}b^{-1}a^{-1}$$

$$a, b, c, . , p, q \in G .$$

Ex. 1. *If every element of a group is its own inverse then show that G is abelian.*

(Lucknow 69; Benares 70; Punjab 67)

Let $a, b \in G$ then $ab \in G$ by closure property.

By given condition $a^{-1}=a$, $b^{-1}=b$, $(ab)^{-1}=ab$

$\therefore$ $ab=(ab)^{-1}=b^{-1}a^{-1}=ba$ Hence G is abelian

Another form

If every element of a group be such that $a^2=e \ \forall \ a \in G$ *then show that G is abelian.*

$a^2=e \Rightarrow a.a=e \Rightarrow a^{-1}=a \quad \forall \ a \in G$

Thus every element of a group is its own inverse and rest as above.

Property 10. An alternative definition of a group.

A set G with a composition is a group iff,

(i) The composition is associative.

(ii) The equations $ax=b$ *and* $ya=b$, $a, b \in G$ *have unique solutions in G.*

(Marthwada 70; Delhi Hon's 70 Rajasthan 66)

We have already defined group in § 3 P. 6 and starting with those axioms we have proved that $ax=b$ and $ya=b$ have unique solutions in the group.

Now we shall start with a set G satisfying the above given conditions and show that it satisfies all the axioms of group given in § 3. This will complete the proof for if and only if, *i.e.* iff. The axiom G_1 of the group, *i.e.* associative composition is the same as condition (1) given above and so what remains to be proved is to show the existence of identity and inverse *i e.* axioms G_2 and G_3 from the given conditions (1) and (2).

We are given that $ax=b$ and $ya=b$ have unique solutions choosing $b=a$ we can say that $ax=a$ and $ya=a$ have unique solutions.

Therefore there must exist elements say e_a and $e_a' \in G$ satisfying the above equations.

$$\therefore \quad ae_a=a \text{ and } e_a'a=a. \qquad \ldots(1)$$

Now $be_a=(ya)\ e_a=y\ (ae_a)=ya=b$ by (1) ...(2)

and $e_a'\ (b)=(e_a')\ (ax)=(e_a'\ a)\ x=ax=b$ by (1) ...(3)

From (2) and (3), we get

$$be_a=b \text{ and } e_a'\ b=b, \forall\ b \in G.$$

Choosing $b=e_a'$ in first and $b=e_a$ in 2nd, we get

$$e_a'e_a=e_a' \text{ and } e_a'e_a=e_a.$$

From above we conclude that $e_a'=e_a=e$ say.

$\therefore$ $be=b$ and $eb=b\ \forall\ b \in G$ from (2) and (3)

Above establishes the existence of identity.

Again $ax=b$ and $ya=b$ have unique solutions, choosing $b=e$ we say $ax=e$ and $ya=e$ have unique solutions.

Hence there must exists unique elements c and $d \in G$ satisfying above.

$$\therefore \quad ac=e \text{ and } da=e. \qquad \ldots(4)$$

Now $ac=e \Rightarrow d\ (ac)=de \Rightarrow (da)\ c=d$, $\because$ e is identity

$$\Rightarrow ec=d \Rightarrow c \quad d.$$

Hence from (4), we get $ac=e$, $ca=e$ $\because$ $d=c$

or $$ac=e=ca.$$

Therefore each a has an unique inverse $c \in G$ and hence axiom G_3 is proved.

Theorem 6. *Prove that a finite set G with an associative composition is a group if the right and left cancellation laws hold in G.* **(Rajasthan M. Sc. 67)**

i.e., $\forall\ a, b, c \in G$

$ab=ac \Rightarrow b=c$ L. C. Law

and $ba=ca \Rightarrow b=c$ R. C. Law.

6967

Prove further that the validity of the cancellation laws does not characterise infinite group but characterises finite groups only. **(Allahabad 70; Lucknow 68; Rajasthan M. Sc. 67; Meerut B Sc. 67)**

Let G be a finite set consisting of n distinct elements only,

$$a_1, a_2, \ldots \ldots, a_n.$$

If a be any of these above elements, then

$$aa_1, aa_2, \ldots, aa_p, \ldots aa_n$$

are all distinct as shown below.

Let $aa_p = aa_r$ if they are not distinct.

But since left cancellation law holds $aa_p = aa_r \Rightarrow a_p = a_r$ which contradicts that G consists of n elements which are distinct.

Therefore $aa_p \neq aa_r$. Hence these n composite elements of the type aa_p are all distinct and they will again be the n given elements of G in some order.

Hence if $a \in G$ then ax where x runs through the elements of G are again n elements of G in some order. In other words any other element $b \in G$ can be written as $b = ax$. For a unique value of x in G [there cannot be two values of x as we have shown that $aa_p = aa_r$].

Hence we can say that the equation $ax = b$ has a unique solution in G.

Similarly by considering the products $a_1a, a_2a, \ldots, a_na$ and by using right cancellation law we can show that the equation $ya = b$ has a unique solution in G. Therefore the composition being associative and the equations $ax = b$ and $ya = b$ having unique solutions, both the conditions of property 10 P. 50 are satisfied and hence the given set is a group

If the set G be infinite then it is not necessarily a group even though the composition is associative and both right and left cancellation laws hold. As an example the set $I^+ = \{1, 2, \ldots, 3\}$

is not a group for multiplication as the inverse does not exist even though it is closed for multiplication which is associative composition and both the cancellation laws hold good.

§ 6. Permutations.

Consider the elements a, b, c of the set $\{a, b, c\}$.

We can arrange these letters a, b, c in the following six manners.

a, b, c; a, c, b; b, a, c; b, c, a; c, a, b; c, b, a.

i.e., there are $\underline{|3} = 6$ ways of arranging them or there are $\underline{|3}$ permutations of the three elements a, b, c. The permutations are written as $P_1, P_2, \ldots$, and we adopt a two line notation to express the permutation.

In the first line we write the elements in their natural order and in the line below it we write them in the order in which they have been rearranged.

i.e. $P_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$ *i.e.* $a \to a, b \to b, c \to c$.

There is no change and this type of permutation is called **identity permutation** and is written as 1.

$$P_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} \text{ i.e. } a \to a, b \to c, c \to b.$$

$$P_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \text{ i.e. } a \to b, b \to a, c \to c,$$

and so on.

Again we could write $P_3 = \begin{pmatrix} c & b & a \\ c & a & b \end{pmatrix}$

which says that $c \to c$, $b \to a$ and $a \to b$, i.e. the two different forms of P_3 do not give a different permutation. From this we conclude that the order of columns in the symbolic representation of a permutation is immaterial so long as the

corresponding elements above and below in the column remain unchanged.

Definition. *A one-one onto mapping of a finite set onto itself is called a permutation, i.e. $f : G \to G$ is called a permutation. The number of elements in the set G is called the degree of permutation.* **(Lucknow 69)**

The set of all permutations of a given set G of n elements is denoted by P_n which will have $n!$ permutations. It is called a symmetric set of degree n.

In other words permutation is the operation of rearranging n distinct objects of a set among themselves.

If $(a_1, a_2, \ldots, a_n)$ be n distinct elements of a set G then the operation of replacing a_1 by b_1, a_2 by $b_2, \ldots, a_n$ by b_n expressed as

$$P=\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{pmatrix}$$

where $b_1, b_2, \ldots, b_n$ are the same n elements as $a_1, a_2, \ldots, a_n$ but in some other order. *i.e.* $f(a_1)=b_1, f(a_2)=b_2, \ldots, f(a_n)=b_n$ *i.e.* each element in the second row is the f-image of the corresponding element of the first row which lies just above it. If they are in the same order then this particular permutation is called Identity permutation.

The arrangement of columns in the above permutation is immaterial and as such P could also be expressed as

$$P=\begin{pmatrix} a_3 & a_n & \ldots & a_1 \\ b_3 & b_n & \ldots & b_1 \end{pmatrix}.$$

Product of two permutations.

Consider the set $S=\{1, 2, 3, 4, 5\}$.

Let α, β, γ be any three permutations of the given set.

$$\alpha=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}, \quad \beta=\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix},$$

$$\gamma=\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}.$$

You may write the above three permutations in any manner you like by taking different arrangements of the numbers in the second line.

$$\alpha\, o\, \beta=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix} o \begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}$$

Now we know that in any permutation the order of columns is immaterial and so we write the permutation β by rearranging the columns in such a manner so that the upper line of β becomes the same as the lower line of α.

$$\therefore \quad \alpha\, o\, \beta=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix} o \begin{pmatrix}2&4&5&1&3\\1&4&5&3&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}=\begin{pmatrix}\text{1st line of } \alpha\\ \text{2nd line of } \beta\end{pmatrix}$$

How ? In the permutation α, $1 \to 2$ and in β, $2 \to 1$.
$\therefore$ In resultant permutation $\alpha\, o\, \beta$, $1 \to 1$. Similarly in α $2 \to 4$ and in β, $4 \to 4$.

$\therefore$ in $\alpha\, o\, \beta$, $2 \to 4$ etc.

We observe that $\alpha\, o\, \beta=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}$ is again a permutation showing there by that in the set of permutations the operation of product of permutations is a binary operation. Also it should be noted that while computing $\alpha\, o\, \beta$ we have to carry out the operation defined by permutation α and then the operation defined by permutation β.

Associative.

$$(\alpha\, o\, \beta)\, o\, \gamma=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix} o \begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}.$$

Rearranging the columns of γ in a manner so that its first line is same as the lower line of $(\alpha\, o\, \beta)$, we get

$$(\alpha\ o\ \beta)\ o\ \gamma=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}\begin{pmatrix}1&4&5&3&2\\4&5&2&1&3\end{pmatrix}.$$

$$(\alpha\ o\ \beta)\ o\ \gamma=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix}=\begin{pmatrix}\text{1st line of } \alpha\ o\ \beta\\ \text{2nd line of } \gamma\end{pmatrix}. \qquad \ldots(1)$$

$$\text{Again } (\beta\ o\ \gamma)=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}o\begin{pmatrix}1&2&3&4&5\\4&3&1&5&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}\begin{pmatrix}3&1&2&4&5\\1&4&3&5&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}.$$

$$\therefore\quad \alpha\ o\ (\beta\ o\ \gamma)=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}o\begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}o\begin{pmatrix}2&4&5&1&3\\4&5&2&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\4&5&2&1&3\end{pmatrix} \qquad \ldots(2)$$

Hence from (1) and (2) we conclude that

$$(\alpha\ o\ \beta)\ o\ \gamma=\gamma\ o\ (\beta\ o\ \gamma),$$

i.e. multiplication composition in the set of permutations is associative.

Identity permutation.

It is a transformation $f: G \to G$ which takes every number of G to itself and this permutation is denoted by I,

$$\therefore\quad I\ \begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}.$$

It is easy to verify that $\alpha\ o\ I \quad I=I\ o\ \alpha$.

Inverse permutation. Since a permutation is one-one onto mapping and as such it is invertible. The inverse of

any permutation α is denoted by α^{-1} and is obtained by interchanging the rows of α.

Thus if.

$$\alpha=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}\text{then }\alpha^{-1}=\begin{pmatrix}2&4&5&1&3\\1&2&3&4&5\end{pmatrix}$$

Clearly $\alpha\ o\ \alpha^{-1}=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=I=\alpha^{-1}\ o\ \alpha$.

Thus the inverse of every permutation exists and belongs to the set.

Permutation multiplication is not commutative in general.

We have shown that

$$\alpha\ o\ \beta=\begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}\ o\ \begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\1&4&5&3&2\end{pmatrix}$$

$$\beta\ o\ \alpha=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}\ o\ \begin{pmatrix}1&2&3&4&5\\2&4&5&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\3&1&2&4&5\end{pmatrix}\ o\ \begin{pmatrix}3&1&2&4&5\\5&2&4&1&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\5&2&4&1&3\end{pmatrix}$$

Hence $\alpha\ o\ \beta\neq\beta\ o\ \alpha$. It is seen that $\alpha\ o\ \beta$ permutation replaces 1 by 1 whereas $\beta\ o\ \alpha$ permutation replaces 1 by 5.

Theorem 4. *The n ! permutations form a group w. r. t. permutation multiplication.* **(Allahabad 69, Meerut B. Sc. 69 B.H.U. 65, Lucknow 68, 69)**

We have proved the theorem above where we have shown that the permutations in the set $S=\{1, 2, 3, 4, 5\}$ satisfy all the axioms of a group. Similarly we can show for n symbols as shown below.

The above group is called a symmetric group on n symbols and of degree n and is denoted by S_n.

or $S_n=\{P : P \text{ is a permutation of degree } n\}$.

Proof. *Let* $S=\{a_1, a_2, \ldots\ldots, a_n\}$, *so that*

$S_n=\{P : P \text{ is a permutation}\}$.

Let $\alpha=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ and $\beta=\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$,

$$\gamma=\begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ d_1 & d_2 & \cdots & d_n \end{pmatrix}$$

be any three permutations of degree n belonging to the set S_n, where b_i, c_i and d_i are same as a_i but in different order.

1. Closure Property. *i e.* product of two permutations is again a permutation belonging to the set S_n.

$$\alpha \circ \beta=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \circ \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

$$=\begin{pmatrix} a_1 & a_2 & & a_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix}$$

which is again a permutation of degree n belonging to the set S_n

The permutation α takes a_1 to b_1 and permutation β takes b_1 to c_1 so that the resulting permutation $\alpha \circ \beta$ takes a_1 to c_1 etc.

2. Associative.

$$(\alpha \circ \beta) \circ \gamma=\begin{pmatrix} a_1 & a_1 & \cdots & a_n \\ c_1 & c_2 & \cdots & c_n \end{pmatrix} \circ \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ d_1 & d_2 & \cdots & d_n \end{pmatrix}$$

$$=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ d_1 & d_2 & \cdots & d_n \end{pmatrix}$$

$$\alpha \circ (\beta \circ \gamma)=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \circ \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ d_1 & d_2 & \cdots & d_n \end{pmatrix}$$

$$=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ d_1 & d_2 & \cdots & d_n \end{pmatrix}$$

Thus $(\alpha\ o\ \beta)\ o\ \gamma=\alpha\ o\ (\beta\ o\ \gamma)$. Hence permutation multiplication is associative.

3. Identity. Consider the permutation

$$I=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \text{ or } =\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

where b_i's are same as a_i's but in some different order and we know that in a permutation we can always change the columns without changing the permutation so that the two permutations written above are same.

Let $\alpha=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$ be any other permutation belonging to S_n.

$$\alpha\ o\ I=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} o \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

$$=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}=\alpha$$

$$I\ o\ \alpha=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$$

$$=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}=\alpha$$

It should be noted that we have taken different forms for I for computing $\alpha\ o\ I$ and $I\ o\ \alpha$. This is done keeping in view that the 2 nd row of first permutation is the same as the first row of second permutation.

Since $\alpha\ o\ I=I\ o\ \alpha=\alpha$ and as such the permutation I is the identity permutation which belongs to S_n.

Inverse Let us denote by α^{-1} the permutation obtained by interchanging the rows in permutation α.

i.e. $\alpha^{-1}=\begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$. Clearly α^{-1} is also a permutation of degree n since b_i's are nothing but a_i's but in a different order.

$$\text{Now } \alpha \, o \, \alpha^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} o \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = I$$

$$\text{and } \alpha^{-1} \, o \, \alpha = \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} o \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

$$= \begin{pmatrix} b_1 & b_2 & \dots & b_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix} = I$$

Since $\alpha \, o \, \alpha^{-1} = \alpha^{-1} \, o \, \alpha =$ as such α^{-1} is the inverse of permutation α and that α^{-1} is again a permutation belonging to S_n. Thus inverse of each permutation exists and belongs to the set.

Rule for writing down the inverse of a permutation α.
Interchange the rows of α.

Non-commutative. As shown on page 57 we can show that multiplication of permutations is not in general commutative.

Hence the set S_n of n ! permutations form a non abelian group.

Note. Students will find it more convenient to choose the set $S = \{1, 2, 3, .., n\}$. Then take any three permutations to be

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 2 & 4 & n & \dots & 3 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 5 & n & 1 & .. & 4 \end{pmatrix},$$

$$\gamma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 7 & 2 & 4 & \dots & n \end{pmatrix}.$$

Any of the above permutation can be so altered by change of columns so that its top row becomes the same as the bottom row of the permutation which preceeds it. Now you prove as above the axioms of a group.

§ 7. Cyclic Permutation.

Definition. ***A permutation which replaces n objects cycli-***

cally is called a cyclic (or circular) permutation of degree n.

Hence the permutation.

$$\alpha=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 5 & 1\end{pmatrix}$$

such that $1 \to 2, 2 \to 3, 3 \to 4, 4 \to 5$ and $5 \to 1$, *i e.* the last number oes to first.

In other words a permutation in which each element in the first line is replaced by the number succeeding it and the last being replaced by first is called a cycilc permutation

Notation. Having understood what we mean by a cyclic permutation we can adopt a one line notation only for a cyclic permutation where $\alpha=(1\ 2\ 3\ 4\ 5)$ would mean a cyclic permutation meaning thereby that each number in the first line is replaced by its successive on the right and the last one by first.

i e. $\alpha=(1\ 2\ 3\ 4\ 5)=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 3 & 4 & 5 & 1\end{pmatrix}$.

Expression for any permutation in terms of cycles

Consider the permutation

$$\beta=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 1 & 2 & 4 & 5\end{pmatrix}=\begin{pmatrix}1 & 3 & 2 & 4 & 5\\ 3 & 2 & 1 & 4 & 5\end{pmatrix}$$

by interchanging the columns.

The above permutation β can be written as $\beta=(1\ 3\ 2)$ which is interpreted as $1 \to 3, 3 \to 2$ and $2 \to 1$, whereas the missing symbols 4 and 5 remain unchanged in the permutation, *i.e.* $4 \to 4$ and $5 \to 5$.

$$\therefore\ \beta=(1\ 3\ 2)=\begin{pmatrix}1 & 3 & 2 & 4 & 5\\ 3 & 2 & 1 & 4 & 5\end{pmatrix}.$$

Thus the permutation β is cyclic and is represented by

cycle (1 3 2) whose length is 3 the number of elements in it.

Again consider the permutation,

$$\gamma=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$$

or $$\gamma=(1\ 2\ 3)\ (4\ 5)$$

as the product of mutually disjoint cycles.

i.e. cycles having no elements common.

Cycle $f=(1\ 2\ 3)=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}$ as permutation.

Cycle $g=\ (4\ 5)=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}$ as permutation.

$\therefore\ fg=.(1\ 2\ 3)\ o\ (4\ 5)$

$$=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}o\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\2&3&1&4&5\end{pmatrix}o\begin{pmatrix}2&3&1&4&5\\2&3&1&5&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=\begin{pmatrix}4&5&1&2&3\\5&4&2&3&1\end{pmatrix}=(4,\ 5)\ (1\ 2\ 3)$$

$$=gf$$

Hence the permutation,

$\gamma=fg=(1\ 2\ 3)\ (4\ 5)=(1\ 2\ 3)\ o\ (4\ 5)$

$$=\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=(4,\ 5)\ (1\ 2\ 3)=gf.$$

Thus we conclude that the product of disjoint cycles is commutative.

Again the permutation.

$$\delta=(2\ 4)\ (3\ 5)=\begin{pmatrix}1&2&4&3&5\\1&4&2&5&3\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\1&4&5&2&3\end{pmatrix}$$

The missing symbol 1 remains unchanged.

Ex. 1. *Prove the following for* 5 *symbols.*

$(1\ 2\ 3) \circ (3\ 1\ 2\ 4) = (1\ 4\ 3\ 2)$.

$$\text{L.H.S.} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 3 & 1 & 2 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 & 1 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 2 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$$

$$= (1\ 4\ 3\ 2).$$

Ex. 2. *Prove that*

$$(3\ 4)\ (1\ 2\ 5) = (3\ 4) \circ (1\ 2\ 5).$$

(3 4) (1 2 5) is the product of mutually disjoint cycles and it can be straight away, written as

$$\begin{pmatrix} 3 & 4 & 1 & 2 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

$$(3\ 4) \circ (1\ 2\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 4 & 3 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

Ex. 3. Powers of cyclic permutation.

Let $\alpha = (1\ 2\ 3\ 4\ 5)$ and α be a cyclic permutation.

$$(1\ 2\ 3\ 4\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

i.e. if we write 1 2 3 4 5 1 2 3 4 5. ...(1)

then the cyclic permutation moves each element by one place in the above line.

Now consider,

$\alpha^2=\alpha\ o\ \alpha=(1\ 2\ 3\ 4\ 5)\ o\ (1\ 2\ 3\ 4\ 5)$

$$=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} o \begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\2&3&4&5&1\end{pmatrix} o \begin{pmatrix}2&3&4&5&1\\3&4&5&1&2\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\3&4&5&1&2\end{pmatrix}$$

i.e. α^2 takes 1 to 3, 2 to 4. 3 to 5, 4 to 1 and 5 to 2,

i.e. it moves each symbol in the line 1 by two places,

i.e. leave the first two elements in line (1) and take the next five.

Also α^2 can be written as

$$\begin{pmatrix}1&3&5&2&4\\3&5&2&4&1\end{pmatrix}=(1\ 3\ 5\ 2\ 4).$$

Similarly $\alpha^3=\alpha\ o\ \alpha^2$ will move each symbol in the line (1) by 3 places, *i.e.* $1\to 4, 2\to 5, 3\to 1, 4\to 2, 5\to 3$, *i.e.* leave the first three elements in line (1) and take the next five.

$$\therefore\quad \alpha^3=\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix}=\begin{pmatrix}1&4&2&5&3\\4&2&5&3&1\end{pmatrix}$$

$$=(1\ 4\ 2\ 5\ 3).$$

Similarly $\alpha^4=\begin{pmatrix}1&2&3&4&5\\4&5&1&2&3\end{pmatrix}=\begin{pmatrix}1&5&4&3&2\\5&4&3&2&1\end{pmatrix}$

$$=(1\ 5\ 4\ 3\ 2).$$

In order to write down α^5 we will have to leave first five places in line (1) and write the next five which are same as first five.

$$\therefore\quad \alpha^5=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=I \text{ (Identity permutation)}$$

$\alpha^6=\alpha^5 \circ \alpha=I \circ \alpha=\alpha$,

$\alpha^{17}=\alpha^{16} \circ \alpha^2=I \circ \alpha^2=\alpha^2$ etc.

Ex. 4. *If* $\alpha=(1\ 2\ 3\ 4\ 5\ 6)$ *prove the following.*

$\alpha^2=(1\ 3\ 5)\ (2\ 4\ 6)$

$\alpha^3=(1\ 4)\ (2\ 5)\ (3\ 6)$

$\alpha^4=(1\ 5\ 3)\ (2\ 6\ 4)$

$\alpha^5=(1\ 6\ 5\ 4\ 3\ 2)$

$\alpha^6=(1)\ (2)\ (3)\ (4)\ (5)\ (6)=I$.

Ex. 5. *Express* $(1\ 3\ 2\ 5) \circ (1\ 4\ 3) \circ (2\ 5\ 1)$ *as the product of disjoint cycles.*

$$=\begin{pmatrix}1&3&2&5&4\\3&2&5&1&4\end{pmatrix} \circ \begin{pmatrix}1&4&3&2&5\\4&3&1&2&5\end{pmatrix} \circ \begin{pmatrix}2&5&1&3&4\\5&1&2&3&4\end{pmatrix}$$

After rearranging the columns

$$=\begin{pmatrix}1&2&3&4&5\\3&5&2&4&1\end{pmatrix} \circ \begin{pmatrix}3&5&2&4&1\\1&5&2&3&4\end{pmatrix} \circ \begin{pmatrix}1&5&2&3&4\\2&1&5&3&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\1&5&2&3&4\end{pmatrix} \circ \begin{pmatrix}1&5&2&3&4\\2&1&5&3&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\2&1&5&3&4\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&5&4\\2&1&5&4&3\end{pmatrix}=(1\ 2)\ (3\ 5\ 4)$$

Similarly $(1\ 4\ 3\ 2) \circ (2\ 4\ 1) \circ (1\ 3\ 5)=(1\ 3\ 4\ 5)$. **Prove.**

§ 9. Transposition.

A cycle of length two of the form (a, b) ***which interchanges only the elements*** a ***and*** b ***and rest of the elements remain unchanged is called a transposition.***

Now we shall show that every cycle and hence every permutation can be expressed as a product of transpositions in many ways.

Consider the set $S=(1\ 2\ 3\ 4)$.

Consider the permutation $(1\ 2\ 3\ 4)=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$

We will change the second line in such a manner that two elements are interchanged and two remain unchanged.

$$\text{or}\quad (1\ 2\ 3\ 4)=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}o\begin{pmatrix}2&1&3&4\\2&3&4&1\end{pmatrix}$$

$$=(1\ 2)\,o\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}$$

$$=(1\ 2)\,o\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}o\begin{pmatrix}3&2&1&4\\3&2&4&1\end{pmatrix}$$

$=(1\ 2)\,o\,(1\ 3)\,o\,(1\ 4)$ *i.e.* 3 transpositions.

Again $(1\ 2\ 3\ 4)=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$

We will change the second line in such a manner that the two elements are interchanged and the remaining two remain unchanged.

$$(1\ 2\ 3\ 4)=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}o\begin{pmatrix}2&1&3&4\\2&3&4&1\end{pmatrix}$$

$$=(1\ 2)\,o\begin{pmatrix}2&1&3&4\\3&1&2&4\end{pmatrix}o\begin{pmatrix}3&1&2&4\\2&3&4&1\end{pmatrix}$$

$$=(1\ 2)\,o\,(2\ 3)\,o\begin{pmatrix}3&1&2&4\\4&1&2&3\end{pmatrix}o\begin{pmatrix}4&1&2&3\\2&3&4&1\end{pmatrix}$$

$$=(1\ 2)\,o\,(2\ 3)\,o\,(3\ 4)\,o\,(4\ 2)\,o\,(1\ 3)$$

Thus the cycle $(1\ 2\ 3\ 4)$ of even length has been expressed as the product of transpositions in two ways and in both of them the number is odd.

Similarly consider the permutation (1 3 5) on the set (1 2 3 4 5) ; then this permutation

$$(1\ 3\ 5)=\begin{pmatrix}1&2&3&4&5\\3&2&5&4&1\end{pmatrix}$$

$$=\begin{pmatrix}1&2&3&4&5\\3&2&1&4&5\end{pmatrix} o \begin{pmatrix}3&2&1&4&5\\3&2&5&4&1\end{pmatrix}$$

$$=(1\ 3)\ o\ (1\ 5).$$

It can also be expressed as (1 5) o (3 5).

Thus the cycle (1 3 5) of odd length has been expressed as the product of transpositions in two ways and in both of them the number is even.

From above example we conclude that a cycle of length n can be expressed as a product of $n-1$ transpositions. It can however be expressed in many other ways but in each case the number will be either odd always or even always.

Theorem. 7. *If a permutation P on n symbols be expressed as the product of r transpositions and also as the product of s transpositions then either both r and s are even or both odd.* **(Benares M. Sc. 1961, 66, 68)**

In other words $r \equiv s \bmod 2$.

i.e. $r-s$ is divisible by 2.

Proof. Let us use the distinct symbols $x_1, x_2, x_3, \ldots, x_n$ and we form the product

$$A=(x_1-x_2)\ (x_1-x_3)\ .\ (x_1-x_n)$$
$$(x_2-x_3)\ldots(x_2-x_n)$$
$$\ldots\ldots\ \ldots\ldots\ldots\ldots$$
$$(x_{n-1}-x_n)$$

For convenience sake let us choose $n=4$ then.

$$A=(x_1-x_2)\ (x_1-x_3)\ (x_1-x_4).\ (x_2-x_3)\ (x_2-x_4)\ (x_3-x_4)$$

Let α be any cyclic permutation (1 3 2) *i.e.* it replaces 1 by 3, 3 by 2 and 2 by 1 whereas 4 remains unchanged. Now by $A\alpha$ we mean the polynomial obtained by changing the suffixes of x in A as prescribed by permutation α *i.e.* suffix 1 is changed to 3, 3 is changed to 2 and 2 is changed to 1.

Thus $A\alpha = (x_3 - x_1)(x_3 - x_2)(x_3 - x_4)(x_1 - x_2)(x_1 - x_4)(x_2 - x_4)$.

Now choosing α to be a transposition say. (1, 2) *i.e.* it changes 1 to 2 and 2 to 1 whereas 3 and 4 remain unchanged.

then $A\alpha = (x_2 - x_1)(x_2 - x_3)(x_2 - x_4)(x_1 - x_3)(x_1 - x_4)(x_3 - x_4)$

$= [-(x_1 - x_2)]\ [(x_2 - x_3)(x_1 - x_3)]\ [(x_2 - x_4)(x_3 - x_4)]$

$[x_1 - x_4] = -A$.

We observe that the factor which involves both 1 and 2 is changed in sign. The factor which does not involve any of the suffix 1 and 2 remain unchanged. The factors which involve either 1 or 2, can be grouped so that the resulting product is not altered *i.e.* to say $x_1 - x_3$ has become $x_2 - x_3$, and $x_2 - x_3$ has become $x_1 - x_3$.

So that $(x_1 - x_3)(x_2 - x_3)$ has become $(x_2 - x_3)(x_1 - x_3)$. Hence the net result of operation in A by a transposition α is to change its sign.

Now a transposition (i, j) where $i < j$ on A has the following effect on A.

(1) Any factor which involves neither x_i nor x_j is unchanged by this transposition (i, j) which interchanges i and j.

(2) The single factor $(x_i - x_j)$ which involves both i and j is changed in sign.

(3) The remaining factors will be of the type which wlll contain either x_i or x_j but not both. Such type of factors be grouped into pairs as

$(x_i-x_k)\,(x_j-x_k)$ when $i<j<k$.

or as $(x_i-x_k)\,(x_k-x_j)$ when $i<k<j$.

or as $(x_k-x_i)\,(x_k-x_j)$ when $k<i<j$.

All the above pairs remain unchanged with the interchanging of i and j. Hence the net effect of transposition on A is to change its sign.

Therefore the effect of permutation P on A is to produce $(-1)^r A$ if P is expressed as the product of r transpositions or to produce $(-1)^s A$ if P is expressed as the product of s transpositions.

But $(-1)^r A=(-1)^s A$ or $(-1)^r=(-1)^s$.

Above will hold only when both r and s are even or both odd.

Definition. Even and odd permutations.

A permutation is called even or odd according as it can be expressed as the product of an even number or of an odd number of transpositions. **(Meerut 68)**

Deduction

(a) *A cycle containing an odd number of symbols is an even permutation whereas a cycle containing an even number of symbols is an odd permutation.*

Cycle of length n=Product of $(n-1)$ transpositions (P. 67). When n is even then $n-1$ is odd and when n is odd then $n-1$ is even.

$\therefore$ Cycle of length (even)=product of odd transpositions.

=odd permutation.

Cycle of length (odd)=product of even transpositions.

$=$Even permutation.

(b) *Identity permutation is always an even permutation.*

$$I=\begin{pmatrix}1&2&3&4&5\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&3&4&5\end{pmatrix}\begin{pmatrix}2&1&3&4&5\\1&2&3&4&5\end{pmatrix}$$

$=(1\ 2)\ (2\ 1)$

$=$Product of two transpositions.

$\therefore$ I is an even permutation.

(c) *Product of two permutations is an even permutation if either both of them are even or both odd and the product is an odd permutation if one is odd and other is even.*

Since $r+s=$even when either both r and s are even or both are odd.

$r+s=$odd when one of them is even and the other is odd.

$P_1=$Product of r transpositions

$P_2=$Product of s transpositions

$\therefore$ $P_1\ P_2=$product of $r+s$ transpositions etc.

(d) *The inverse of an even permutation is an even permutation and the inverse of an odd permutation is an odd permutation.*

$PP^{-1}=I$ and I is an even permutation by (b)

By (c) above is possible if either both P and P^{-1} are even or both odd. Since P is even therefore P^{-1} is also even.

§ **10.** *To prove that of the n ! permutations on n symbols,* $\frac{n!}{2}$ *are even and* $\frac{n!}{2}$ *are odd.* **(Luck. 69; Meerut 68)**

Let us suppose that out of n ! permutations $E_1, E_2, \ldots E_r$ are r even permutations and $O_1, O_2, \ldots O_s$ are odd permutations and because a permutation is either even or odd but not both so that $r+s=n$!

To prove that $r=s=\frac{n!}{2}$.

Take t to be any transposition which itself is a permutation expressed as single transposition and as such t is an odd permutation and the multiplication of all the even permutations by t will change them to odd and odd permutations to even.

Thus $t E_1, t E_2, \ldots\ldots, t E_r$ are r odd permutations.

and $t O_1, t O_2, \ldots\ldots, t O_s$ are s even permutations.

The above two sets of permutations will not have any permutation common since an odd permutation can not be an even permutation.

Further of the set of odd permutations $t E_i$ all will be distinct for if not then let $t E_i = t E_j \Rightarrow E_i = E_j$ by Cancellation Law.

Similarly $t O_i \neq t O_j$.

Hence we conclude that of all the r odd permutations which are distinct *i.e.*, $t E_1, \ldots\ldots, t E_r$ should be the same as the given s odd permutations $O_1, O_2 \ldots O_s$ in some different order. Similarly of all the s even permutations which are distinct *i.e.*, $t O_1, t O_2, \ldots\ldots, t O_s$ should be same as the given r even permutations $E_1, E_2, \ldots\ldots, E_r$.

Hence we conclude that $r=s$ but since $r+s=n!$

$$\therefore \quad r=s=\frac{n!}{2}$$ **Proved.**

Theorem. 8. *To prove that the* $\frac{n!}{2}$ *even permutations form a finite non-abelian group with respect to permutation multiplication.* **(Gorkhpur 70; Luck. 69; B. H. U. 70)**

Proof : Closure property

Let α and β be two even permutations so that α and β are expressible as the product of r and s transpositions where

both r and s will be even. Henee the product $\alpha\ o\ \beta$ is expressible as the product of $r+s$ *i.e.* even transpositions and hence $\alpha\ o\ \beta$ is also an even permutation.

Note. This closure property will not hold good for the set of $\frac{n!}{2}$ odd permutations because when both r and s are odd then $r+s$=even *i.e.* $\alpha\ o\ \beta$ will be an even permutation when both α and β are odd permutations.

Associative. Again we have already seen and can be shown as on P. 55 or 58 that permutation multiplication is associative.

Identity. I is the identity permutation which we have shown on P 70 (b) to be an even permut ation and as such it belongs to the set of even permutations.

Also $If=fI=f$. $\forall\ f \in$ set

Inverse. Again if f be an even permutation then f^{-1} is also an even permutation because $ff^{-1}=$I and I is also an even permutation and we know from (c) P. 70 that product of two permutations is an even permutation if either both are even or both odd. But f is even $\therefore f^{-1}$ is also even. Hence f^{-1} is an even permutation.

Therefore all the axioms of a group are satisfied. We have also shown that permutation multiplication is not commutative and as such the above set of $\frac{n!}{2}$ even permutations is finite non abelian group :—

Alternating group on n symbols :

The above group of $\frac{n!}{2}$even permutations is called an alternating group on n symbols w.r.t. permutation multiplication.

Exercise 3

Ex. 1. *Prove that the set A_3 consisting of three permutations I, (a, b, c), (a, c, b) on three symbols a, b, c forms a finite abelian group w. r. t. permutation multiplication. Prepare a composition table.*

Let $\alpha_1 = I = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$, $\alpha_2 = (a, b, c) = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$

and $\alpha_3 = (a \quad c \quad b) = \begin{pmatrix} a & c & b \\ c & b & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$

clearly $\alpha_1 \, o \, \alpha_2 = \alpha_2$, $\alpha_1 \, o \, \alpha_3 = \alpha_3$ as α_1 is identity permutation

$$\alpha_2 \, o \, \alpha_3 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} o \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} o \begin{pmatrix} b & c & a \\ a & b & c \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I = \alpha_1$$

$$\alpha_3 \, o \, \alpha_3 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} o \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} o \begin{pmatrix} b & \blacksquare & a \\ c & \blacksquare & b \end{pmatrix}$$

$$= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$

$$= \begin{pmatrix} a & c & b \\ c & b & a \end{pmatrix} = (a \quad c \quad b) = \alpha_3.$$

Similarly we can show that

$$\alpha_3 \, o \, \alpha_1 = \alpha_3, \; \alpha_3 \, o \, \alpha_2 = \alpha_1, \; \alpha_3 \, o \, \alpha_3 = \alpha_2$$

Hence we have the following composition table.

o	α_1	α_2	α_3
α_1	α_1	α_2	α_3
α_2	α_2	α_3	α_1
α_3	α_3	α_1	α_2

1. Product of any two permutations is again a permutation belonging to the set and hence closure property is satisfied.

2. Composition is clearly associative because

$$(\alpha_1 \circ \alpha_2) \circ \alpha_3 = \alpha_2 \circ \alpha_3 = \alpha_1$$
$$\alpha_1 \circ (\alpha_2 \circ \alpha_3) = \alpha_1 \circ (\alpha_1) = \alpha_1.$$

3. α_1 is the identity element.

4. Each element has inverse as is clear from the composition table, *e.g.*, $\alpha_1^{-1} = \alpha_1 \quad \alpha_2^{-1} = \alpha_3 \quad \alpha_3^{-1} = \alpha_2$.

5. Since each row is identical with the corresponding column therefore the composition is commutative

Hence the given set is a finite abelian group of order 3.

Ex. 2. *Prove that the four permutations,*

I, (ab), (cd) *and* $ab)\ (cd)$ *on four symbols* a, b, c, d. *form a finite abelian group w.r.t, permutation multiplication.*

$$I = (a)\ (b)\ (c)\ (d) = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} = \alpha_1.$$

$$(ab) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} = \alpha_2$$

$$(cd) = \begin{pmatrix} a & b & c & d \\ a & b & d & c \end{pmatrix} = \alpha_3,$$

$$(ab)\ (cd) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} = \alpha_4 \text{ say}$$

We shall prepare a composition table as under.

α_1 is identity permutation so that

$$\alpha_1 \circ \alpha_1 = \alpha_1,\ \alpha_1 \circ \alpha_2 = \alpha_2 \circ \alpha_1 = \alpha_2,\ \alpha_3 \circ \alpha_1 = \alpha_1 \circ \alpha_3 = \alpha_3,$$
$$\alpha_4 \circ \alpha_1 = \alpha_1 \circ \alpha_4 = \alpha_4$$

$$\alpha_2 \circ \alpha_2 = (ab) \circ (ab) = \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} \circ \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix}$$
$$= \begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} \begin{pmatrix} b & a & c & d \\ a & b & c & d \end{pmatrix}$$
$$= \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} = I = \alpha_1.$$

$$\alpha_2 \, o \, \alpha_3 = (ab) \, o \, (cd) = (ab)\,(cd) = \alpha_4 = \alpha_3 \, o \, \alpha_2$$
$$\alpha_2 \, o \, \alpha_4 = (ab) \, o \, (ab)\,(cd) = (a)\,(b)\,(cd) = (cd) = \alpha_3.$$

In the first $a \to b$ and in second $b \to a$

$\therefore$ $a \to a$ in resultant.

Similarly $b \to a$. and $a \to b$ $\therefore$ $b \to b$ in resultant.

Similarly $\alpha_4 \, o \, \alpha_2 = \alpha_3$. and $\alpha_3 \, o \, \alpha_4 = (cd) \, o \, (ab)\,(cd) = \alpha_2 = \alpha_1 \, o \, \alpha_3$.

Hence the composition table is as below

o	α_1	α_2	α_3	α_4
α_1	α_1	α_2	α_3	α_4
α_2	α_2	α_1	α_4	α_3
α_3	α_3	α_4	α_1	α_2
α_4	α_4	α_3	α_2	α_1

Comparing with the composition tables of Ex.21 or Ex.22 P. 27-29 we find that they are identical and hence with the same arguments as on P. 27-29 we can say that the given set constitutes a finite abelian group w.r.t. permutation multiplication.

$(\alpha_1)^{-1} = \alpha_1$, $(\alpha_2)^{-1} = \alpha_2$, $(\alpha_3)^{-1} = \alpha_3$, $(\alpha_4)^{-1} = \alpha_4$ etc.

Ex. 3. *Show that the set of all permutations on three symbols a, b, c is a finite non abelian group w.r.t. permutation multiplication as composition.* **(Benares M. Sc 63)**

We can arrange the three letters a, b, c in the following six ways.

(1) $(a\ b\ c)$, (2) $(a\ c\ b)$, (3) $(b\ a\ c)$ (4) $(b\ c\ a)$, (5) $(c\ a\ b)$, (6) $(c\ b\ a)$ *i.e.* the six permutations are

$$\alpha_1 = \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} = I, \quad \alpha_2 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = (b\ c)$$

$$\alpha_3 = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} = (a, b) \quad \alpha_4 = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (a\ b\ c)$$

$$\alpha_5=\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix}=\begin{pmatrix}a & c & b\\ c & b & a\end{pmatrix}=(a\ c\ b)$$

$$\alpha_6=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}=(a\ c)$$

$$\therefore \quad G=\{\alpha_1, \alpha_2,\ldots,\alpha_6\}.$$

We shall prepare a composition table as under

α_1 is identity permutation

$$\therefore \quad \alpha_1 \circ \alpha_1=\alpha_1,\ \alpha_1 \circ \alpha_2=\alpha_2,\ldots,\alpha_1 \circ \alpha_6=\alpha_6.$$

Again $\alpha_2 \circ \alpha_2=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & c & b\\ a & b & c\end{pmatrix}$

$$=\begin{pmatrix}a & b & c\\ a & b & c\end{pmatrix}=\alpha_1$$

$$\alpha_2 \circ \alpha_3=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & c & b\\ b & c & a\end{pmatrix}$$

$$=\begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}=\alpha_4$$

$$\alpha_2 \circ \alpha_4=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & b & c\\ b & c & a\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & c & b\\ b & a & c\end{pmatrix}$$

$$=\begin{pmatrix}a & b & c\\ b & a & c\end{pmatrix}=\alpha_3.$$

$$\alpha_2 \circ \alpha_5=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & c & b\\ c & b & a\end{pmatrix}=\begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}=\alpha_6$$

$$\alpha_2 \circ \alpha_6=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & b & c\\ c & b & a\end{pmatrix}=\begin{pmatrix}a & b & c\\ a & c & b\end{pmatrix} \circ \begin{pmatrix}a & c & b\\ c & a & b\end{pmatrix}$$

$$\begin{pmatrix}a & b & c\\ c & a & b\end{pmatrix}=\alpha_5$$

Similarly we can find other composite permutations and we have the following composition table

o	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_1	α_2	α_3	α_4	α_5	α_6
α_2	α_2	α_1	α_4	α_3	α_6	α_5
α_3	α_3	α_5	α_1	α_6	α_2	α_4
α_4	α_4	α_6	α_2	α_5	α_1	α_3
α_5	α_5	α_3	α_6	α_1	α_4	α_2
α_6	α_6	α_4	α_5	α_2	α_3	α_1

Axioms of group

I. Closure. All the composite permutations are again permutations which belong to set G which therefore is closed for the composition 'multiplication of permutation'.

Associative. We know that multiplication of permutations is always associative. Consider from the table.

$$(\alpha_2 \, o \, \alpha_3) \, o \, \alpha_4 = (\alpha_4 \, o \, \alpha_4) = \alpha_5$$

$$\alpha_2 \, o \, (\alpha_3 \, o \, \alpha_4) = (\alpha_2 \, o \, \alpha_6) = \alpha_5$$

$$\therefore \quad (\alpha_2 \, o \, \alpha_3) \, o \, \alpha_4 = \alpha_2 \, o \, (\alpha_3 \, o \, \alpha_4)$$

Identity. Clearly α_1 is the identity permutation.

$$\text{as} \quad \alpha_1 o \, \alpha_5 = \alpha_5 \, o \, \alpha_1 = \alpha_5$$

Inverse. Since identity permutation α_1 is present in each row of the table showing that the inverse exists.

The inverse of α_1 is α_1, of α_2 is α_2 of α_3 is α_3, of α_4 is α_5 of α_5 is α_4, of α_6 is α_6.

Rule. To find the inverse of say α_5 look to the row headed by α_5 and see the identity element α_1 then the element at the head of this column which is α_4 is the inverse of α_5 from the table.

$$\alpha_5 \, o \, \alpha_4 = \alpha_1 = \alpha_4 \, o \, \alpha_5.$$

Not Commutative. From the table. $\alpha_2 \, o \, \alpha_3 = \alpha_4$ whereas $\alpha_3 \, o \, \alpha_2 = \alpha_5$ so that $\alpha_2 \, o \, \alpha_3 \neq \alpha_3 \, o \, \alpha_2$.

Hence G finite non-abelian group of order 6 with respect to permutation multiplication.

§ 11. Integral powers of an element :

Let G be a group with binary operation o **(ordinary multiplication)** and a be any element of the group, then by general associative law the product $a\ o\ a\ o\ a\ o\ a$.....a to m factors is independent of the manner in which these factors be grouped. This product of m factors will be denoted by a^m.

Thus for **multiplicatioa composition :**

(1) $a\ o\ a\ o\ a$ .....a, m factors $=a^m$.

Also we define

(2) $a^0=e$ where e is the identity element.

(3) Again when m is a $-$ive integer say $m=-n$ where n is $+$ive integer then we define $a^m=a^{-n}=(a^n)^{-1}$ and using this deflnion we shall prove that $\mathbf{a^{-n}=(a^{-1})^n}$.

Now $a^{-n}=(a^n)^{-1}$ by def.$=(a\ o\ a\ o\ a$..... n factors$)^{-1}$

by def.

$=(a^{-1}\ o\ a^{-1}\ o\ a^{-1}$.....$n$ factors$)=(a^{-1})^n$.

$\because$ $[a\ b\ c]^{-1}=c^{-1}\ b^{-1}\ a^{-1}$. Prop. 9 Page 49

$\therefore$ $a^{-n}=(a^{-1})^n$.

or $a^m=a^{-n}\cdot(a^n)^{-1}=(a^{-1})^n$ where $m=-n$.

Again for additive composition :

(1) $a+a+a+$ .....m factors $=ma$.

Also we define.

(2) $0\ a=0$ (identity of additive group) where 0 on the left is the zero integer)

(3) when m is $-$ive say $-n$ then

$ma=-(na)=n(-a)$.

Hence we have defined both a^n and ma when m is 0, $+$ive or $-$ive integer ;

Laws of Indices. Multiplicative composition

(*i*) $a^r\ o\ a^s=a^{r+s}$, (*ii*) $a^{rs}=(a^r)^s$. $\forall$ $a \in G$ and $r, s \in I$

Laws of multiples. Additive composition

$(m+n)\,a=ma+na$, $m\,(na)=(mn)\,a$, $\forall\ a \in G$, $m, n \in I$

§ 12. Order of an element of a group.

Definition. *Let G be a group and a be any element of it. The order of this element a is defined as* **the least +ive integer n such that $a^n=e$.**

In case no such +ive integer n exists such that $a^n = e$ then we say that the element a is **of infinite or of zero order.**

(Kanpur 69; Meerut 70, B. H. U. 70; Gorakhpur 70; Lucknow 66, 67, 69; Marthwada 70; Raj. M. Sc, 69)

Notation. The order of a is m is expressed as $o\,(a)=m$. *i.e.* $a^m=e$ where m is the least +ive integer satisfying the above relation.

For additive notation. We shall say $ma=e$ in place of $a^m=e$.

The order of identity element.

The order of identity element e of the group is 1 and in fact this is the only element of the group whose order is 1 because if $a \neq e$ be an element of order 1 then $a^1=e$ by def. which is a contradiction.

Cor. Let $o\,(a)=m$ then $a^m=e$. Also if $a^p=e$ then $m \leqslant p$ as m is the least +ive integer such that $a^m=e$.

Illustration.

1. Consider the group $(1, \omega, \omega^2)$ for multiplicative composition. 1 is the identity and its order is 1. Also $\omega^3=1$ (identity). Therefore order of element ω is 3. Again $(\omega^2)^3=\omega^6=1$ (identity). Therefore order of element ω^2 is 3 as 3 is the least +ive integer such that $(\omega^2)^3=1$.

2. Again consider the multiplicative group consisting of four fourth roots of unity, *i.e.* $\{1, -1, i, -i\}$. (Ex. 8, 9 P. 15)

The identity is 1. Also $(1)^1=1$, $(-1)^2=1$, $(i)^4=1$, $(-i)^4=1$.

Hence the order of the elements $1, -1, i$ and $-i$ are 1, 2, 4, 4 respectively.

3. Again consider the cyclic group (To the discussed later) $(a, a^2, a^3, a^4, a^5, a^6)$, where $a^6=e$ (identity).

$(a)^6=e$, $(a^2)^3=a^6=e$, $(a^3)^2=a^6=e$, $(a^4)^3=a^{12}=e$,

$(a^5)^6=a^{30}=e$, $(a^6)^1=a^6=e$.

Hence the orders of the elements are respectively.

6, 3, 2, 3, 6, 1

4. *Find the order of each of the element of group* $G=\{0, 1, 2, 3, 4, 5\}$ **[Ex. 25. P. 33]**

the composition being addition modulo 6.

In additive notation the order of an element is that least +ive integer m such that $ma=e$

Here 0 is the identity and its order is 1.

Now $6(1)=6=0$ under addition modulo 6 $\therefore o(1)=6$

$3(2)=6=0$,, ,, ,, $\therefore o(2)=3$

$2(3)=6=0$,, ,, ,, $\therefore o(3)=2$

$3(4)=12=0$,, ,, ,, $\therefore o(4)=3$

$6(5)=30=0$,, ,, ,, $\therefore o(5)=6$

5. Consider the **infinite** multiplicative group of non zero rational numbers. In this group the order of 1 is 1 and of -1 is 2 as $(-1)^2=1$ (identity). But the order of rest of the elements is infinite because for any other element a there will not exist a least +ive integer n such that $a^n=e=1$ (identity).

Hence we conclude that in an infinite group there may exist elements whose order is finite and the order of the r st be infinite. But in a finite group the order of each element is finite, as is proved in the following theorem,

§ 13. Certain Theorems on the order of an element of a group.

Theorem 9. *The order of every element* **of a finite group is finite.**

Let G be a finite group and a be any element of it. Now consider all the +ive integral powers of a, *i.e.*

$$a, a^2, a^3, \ldots$$

Each one of these powers is again an element of the group. But since G is a finite group, therefore all these integral powers of a cannot be different. Hence we suppose that an element a^q, where q is greater than p is the same as the element a^p, *i e.* $a^q = a^p$, $q > p$ or $q-p =$ +ive.

Now $a^q = a^p \Rightarrow a^q a^{-p} = a^p a^{-p} \Rightarrow a^{q-p} = a^r = e$

or $$a^r = e.$$

putting $q-p=r$ another integer which is +ive.

Thus there exist a +ive intager r such that $a^r = e$.

Now if $o(a) = n$ then $a^n = e$ where by definition n is the least positive integer satisfying the above relation

Since $a^r = e \quad \therefore \; n \leqslant r \quad$ or $n \leqslant q-p$.

But q and p are both finite $\therefore$ $q-p$ is also finite and consequently n being less than $q-p$ is also finite. Hence the order of every element of a finite group is finite.

Theorem 10. *The order of any power of an element a of a group cannot exceed the order of a, i.e., order of* a^s *cannot be greater than the order of a.* **(Lucknow 67, 69)**

Let a be any element of a group and a^s be an integral power of this element. Let n and m be the orders of these two elements therefore $a^n = e$ and $(a^s)^m = e$ by definition where n and m are the least +ive integers satisfying the above relations.

Now $(a^s)^n = (a^n)^s = e^s = e. \quad \because \quad a^n = e.$

Also $(a^s)^m=e$ **where m is the least +ive integer as** m **is** the order of a^s.

Hence we conclude that $n \geqslant m$ or $m \leqslant n$. In other words m the order of a^s can not be greater than n the order of a.

Theorem 11. *The order of an element a of a group is the same as the order of its inverse element* a^{-1}.

(Lucknow 68; Meerut B. Sc. 68)

Let n and m be the orders of a and a^{-1}, so that $a^n=e$ and $(a^{-1})^m=e$.

We shall show that $n=m$ by establishing that $n \leqslant m$ and $m \leqslant n$ and both these results will imply that $n=m$.

$o(a)=n \Rightarrow a^n=e \Rightarrow (a^n)^{-1}=e^{-1} \Rightarrow (a^{-1})^n=e.$

But $(a^{-1})^m=e$ where m is order of a^{-1}

$\therefore \quad m \leqslant n$ (cor. P. 79)

Again $o(a^{-1})=m \Rightarrow (a^{-1})^m=e \Rightarrow (a^m)^{-1}=e \Rightarrow a^m=e.$

$[\because \quad d^{-1}=e \Rightarrow d=e]$

But $a^n=e$ where n is the order of a

$\therefore \quad n \leqslant m$ ...(2)

Hence from I and 2 we conclude that $m=n$.

Also if the order of a is infinite then the order a^{-1} can not be finite because if $o(a^{-1})=$finite$=m$ say
then $(a^{-1})^m=e \Rightarrow (a^m)^{-1}=e \Rightarrow a^m=e.$
and hence $n \leqslant m$ or $o(a) \leqslant m$ where m is finite or $o(a)=$finite which is a contradiction. Hence if $o(a)=$infinite then $o(a^{-1})$ is also infinite.

Theorem 12. *If the element a is of order n, i.e.* $a^n=e$, *then* $a^m=e$ *iff* $m=nq$. **(Lucknow 69)**

Now since $a^n=e$, $a^m=e$ therefore $m \geqslant n$ because n

being the order of a is the least +ive integer satisfying the relation $a^n=e$.

Let $m=nq+r$ where $0 \leqslant r < n$.

Now $a^m=e \Rightarrow a^{nq+r}=e \Rightarrow (a^n)^q . a^r=e$

$\Rightarrow a^r=e$ [$\because$ $a^n=e$].

But this is not possible because r is less than n the order of a and we know that there can not be any integer r less than n such that $a^r=e$. Hence r must be zero so that $m=nq$.

Again if $m=nq$; then $a^m=a^{nq}=(a^n)^q=e^q=e$. [$\because$ $a^n=e$]

Hence $a^m=e$ iff $m=nq$

Theorem 13. *The order of any element a of a group is the same as that of $x^{-1}ax$ where x is any element of the group.* **(Gorakhpur 70)**

Let the order of element a be n, so that

$$a^n=e. \qquad \ldots(1)$$

Now consider

$$(x^{-1}ax)^2=(x^{-1}ax)\,(x^{-1}ax)=x^{-1}a\,(xx^{-1})\,ax$$
$$=x^{-1}aeax=x^{-1}a^2x.$$

In general we have

$$(x^{-1}ax)^n=x^{-1}a^n x=x^{-1}ex \text{ by } (1)$$
$$=x^{-1}x=e$$

Hence n will be order of $x^{-1}ax$ if we show that n is the least +ive integer satisfying the above relation.

Now if m is any other +ive integer less than n then

$$(x^{-1}ax)^m=x^{-1}a^m x \neq e$$

because $a^m \neq e$ as n is the order of a and there cannot be any other +ive integer m less than n such that $a^m=e$.

Therefore n is the least +ive integer such that

$$(x^{-1}ax)^n=e$$

and hence its order is n.

Cor. *Prove that order of ab and ba are the same.*

Now $ab=b^{-1}(ba)\ b$ and as such by Theorem 13, *i.e.* orders of a and $x^{-1}ax$ are same we conclude that the order of ab and ba are the same.

Theorem 14. *If a is of order n and p is prime to n then the order of a^p is also n.*

Let us suppose that the order of a^p is m, then by Theorem 10.

$$m \leqslant n. \qquad \ldots(1)$$

Again since p is prime to n there exists integers x and y such that

$$px+ny=1.$$

$$\therefore\quad a=a^{px+ny}=a^{px}.a^{ny}=(a^p)^x.(a^n)^y=(a^p)^x,\quad \because\ a^n=e.$$

Hence we have expressed a as a power of a^p so that by Theorem 10, order of a is less than order of a^p

i e. $$n \leqslant m. \qquad \ldots(2)$$

From (1) and (2) we conclude that $m=n$, *e.g.* if the order of a be 3, *i.e.* $a^3=e$, then the order of a^7 will also be 3 because $(a^7)^3=(a^3)^7=e^7=e$.

Exercise 4

1. *If G is a group of even order, prove that there exists an element $a\neq e$ s.t, $a^2=e$.*

The number of elements in G are even as it is of even order. Also in a group each element is inversible and its inverse belongs to the set. Thus n elements and n inverses will make $2n$ elements. Out of these n elements $e^{-1}=e$ and thus we will have only $2n-1$ elements which would mean that the group is of odd order. Hence there must exist at least one more element (In general odd elements) whose inverse is the element itself so that we have in all even number of elements.

Hence $a^{-1}=a \Rightarrow a\,a^{-1}=a\,a \Rightarrow e=a^2$

2. *Give an example of an infinite group each element of which is of finite order.* **(Poona 70)**

Let $G=\{n$th roots of unity $\forall\ n \in N\}$

In other words elements of G are square roots, cube roots, fourth roots nth..... roots of unity and so on. It is an infinite group with 1 as identity. If ω be one of the elements then $\omega^2=1$, $\omega^3=1$, $\omega^4=1$, $\omega^5=1$... according as ω is square root cube root, fourth root and so on of unity and clearly the order of ω is finite. But ω is arbitrary and hence order of every element of the set is finite.

3. *Distinguish between the order of a group and order of an element of a group.*

(Gorakhpur 70; Meerut 70)

The order of a group stands for the number of elements in it whereas the order of an element a of a group G is the least +ive integer n such that $a^n=e$ where e is the identity element.

4. *If the order of every element of a group (except the identity element) be two then the group is abelian,*

Or

If every element of a group is its own inverse then G is abelian. **(Punjab 67)**

Let a and b be any two elements of a group of order 2 such that $a^2=e$, $b^2=e$.

Now ab will again be an element of the group therefore $(ab)^2=e$ also and we have to show that $ab=ba$ *i.e.* G is abelian.

$(ab)^2=e \Rightarrow (ab)\,(ab)=e \Rightarrow a\,(ba)\,b=e$

$\Rightarrow a\,[a\,(ba)\,b]\,b=aeb \Rightarrow (aa)\,(ba)\,(bb)=ab$

$\Rightarrow a^2\,(ba)\,b^2=ab \Rightarrow e\,(ba)\,e=ab$ $\quad \because\ a^2=e,\ b^2=e$

$\Rightarrow ba=ab.$

Hence G is abelian.

Alternative Method.

$a^2=e \Rightarrow a.a=e \Rightarrow a^{-1}=a.$ ...(1)

Similarly $b^2=e \Rightarrow b^{-1}=b.$ ...(2)

Again $ab \in G \therefore (ab)^2=e \Rightarrow (ab)^{-1}=ab$

$\Rightarrow b^{-1}a^{-1}=ab \Rightarrow ba=ab \Rightarrow G$ is abelian.

5. *If* $b^{-1}a^{-1}ba=e \ \forall \ a, b \in G$ *then the group* G *is abelian.*

$b^{-1}a^{-1}ba=e \Rightarrow (b^{-1}a^{-1})(ba)=e$

$\Rightarrow (b^{-1}a^{-1})^{-1}=ba$ $\because$ $ab=e \Rightarrow a^{-1}=b.$

$\Rightarrow (a^{-1})^{-1}(b^{-1})^{-1}=ba$ $\because$ $(ab)^{-1}=b^{-1}a^{-1}$

$\Rightarrow ab=ba$ $\because$ $(a^{-1})^{-1}=a.$

Hence G is an abelian group.

6. *Prove that* $(ab)^2=a^2b^2 \Leftrightarrow G$ *is abelian where* $a, b \in G.$

Ist. Case. $(ab)^2=a^2b^2$ to prove $ab=ba$ *i.e.* G is abelian.

$(ab)^2=a^2b^2 \Rightarrow (ab)(ab)=(aa)(bb)$

$\Rightarrow a(ba)b=a(ab)b$ by associative law.

$\Rightarrow ba=ab$ by cancellation laws,

Hence G is abelian.

2nd Case. G is abelian *i.e.* $ab=ba$, to show that $(ab)^2=a^2b^2$

$(ab)^2=(ab)(ab)=a(ba)b=a(ab)b$ $\because$ $ba=ab$

$=(aa)(bb)=a^2b^2.$ **Proved.**

7. $a^2=a \Rightarrow a=e \ \forall \ a \in G$

$a^2=a \Rightarrow aa=a \Rightarrow (aa)a^{-1}=aa^{-1}$

$\Rightarrow a(aa^{-1})=e \Rightarrow ae=e \Rightarrow a=e.$

8. *Prove that if in a group the elements* a *and* b, *commute then*

(*i*) a^{-1}, b^{-1}, (*ii*) a, b^{-1}, (*iii*) a^{-1}, b *also commute.*

(*i*) Given $ab=ba \Rightarrow (ab)^{-1}=(ba)^{-1} \Rightarrow b^{-1}a^{-1}=a^{-1}b^{-1}$
i.e. a^{-1}, b^{-1} commute.

(*ii*) $ab=ba \Rightarrow b^{-1}(ab)b^{-1}=b^{-1}(ba)b^{-1}$
$\Rightarrow (b^{-1}a)(bb^{-1})=(b^{-1}b)(ab^{-1})$
$\Rightarrow (b^{-1}a)e=e(ab^{-1}) \Rightarrow b^{-1}a=ab^{-1}$.

i.e. a, b^{-1} commute.

(*iii*) $ab=ba \Rightarrow a^{-1}(ab)a^{-1}=a^{-1}(ba)a^{-1}$
$\Rightarrow (a^{-1}a)(b\,a^{-1})=(a^{-1}b)(a\,a^{-1})$
$\Rightarrow e(b\,a^{-1})=(a^{-1}b)e \Rightarrow b\,a^{-1}=a^{-1}b$

i.e. a^{-1}, b commute.

9. *If a and b are any elements of a group G then* $(ba\,b^{-1})^n=ba^n\,b^{-1}$ *for any integer n.*

Case I. $n=0$ then $(ba\,b^{-1})^n=(ba\,b^{-1})^0=e$ by definition.
Also $ba^n\,b^{-1}=ba^0\,b^{-1}=be\,b^{-1}=bb^{-1}=e$
$\therefore \quad (ba\,b^{-1})^n=b\,a^n\,b^{-1}$

Case II. $n>0$ $(ba\,b^{-1})^1=ba\,b^{-1}=b\,a^1\,b^{-1}$

Hence the result is true for $n=1$ and let us suppose that result is true for $n=p$.

i.e. $(ba\,b^{-1})^p=b\,a^p\,b^{-1}$

then $(ba\,b^{-1})^{p+1}=(ba\,b^{-1})^p(ba\,b^{-1})=(b\,a^p\,b^{-1})(ba\,b^{-1})$.
$=b\,a^p(b^{-1}\,b)\,ab^{-1}=ba^p\,ea\,b^{-1}$
$=b\,a^p.a\,b^{-1}=b\,a^{p+1}\,b^{-1}$

Thus we observe that the result is true for $n=p+1$ also and it was found to be true for $n=1$. Therefore by induction the result holds good for all values of n which are greater than zero.

Case III. $n<0$ say $n=-m$ where m is +ive.
$(b\,a\,b^{-1})^n=(b\,a\,b^{-1})^{-m}=[(b\,a\,b^{-1})^m]^{-1}=(b\,a^m\,b^{-1})^{-1}$ by case II
$=(b^{-1})^{-1}(a^m)^{-1}\,b^{-1}=b\,a^{-m}\,b^{-1}=b\,a^n\,b^{-1}$.

Hence $(b\ a\ b^{-1})^n = b\ a^n\ b^{-1}$ for all integral values of n.

10. *Prove that if G is an abelian group then for all $a, b \in G$ and for all integers n, $(ab)^n = a^n\ b^n$.*

Case I. $n=0$ $(ab)^n=(ab)^0=e$. by definition.

Also $a^n\ b^n=a^0\ b^0=ee=e$. $\therefore$ $(ab)^n=a^n\ b^n$

Case II. $n > 0$ and G is abelian.

$(ab)^1=ab=a^1\ b^1$. *i.e.* the result holds good for $n=1$ and let us suppose that it holds good for $n=p$ so that $(ab)^p=a^p\ b^p$.

Now $(ab)^{p+1}=(ab)^p\ (ab)=(a^p\ b^p)\ (ab)$.

$=a^p\ (b^p\ a)\ b=a^p\ (a\ b^p)\ b$. $\because$ $b^pa=a\ b^p$ as G is abelian.

$=(a^pa)\ (b^p\ b)=a^{p+1}\ b^{p+1}$.

Hence the result is true for $n=p+1$ and it was found to hold good for $n=1$.

Therefore by induction result holds good for all +ive integers n.

Case III. $n < 0$. Let $n=-m$ when m is +ive.

$(ab)^n=(ab)^{-m}=[(ab)^m]^{-1}=[a^m\ b^m]^{-1}$ by case II

$=(b^m\ a^m)^{-1}$ $\because$ G is abelian *i.e.* $a^m\ b^m=b^ma^m$

$=(a^m)^{-1}\ (b^m)^{-1}=a^{-m}\ b^{-m}=a^n\ b^n$.

Hence the result holds good for all values of n.

11. *If G is a group such that $(ab)^n=a^n\ b^n$ for three consecutive integers n for all a, b in G, show that G is abelian*

(Meerut M. Sc. 1969)

Let us choose the three consecutive integers to be $p, p+1, p+2$ so that $(ab)^p=a^p\ b^p$, $(ab)^{p+1}=a^{p+1}\ b^{p+1}$, $(ab)^{p+2}=a^{p+2}\ b^{p+2}$.

Now $(ab)^{m+2}=(ab)^{m+1}\ (ab)$

$\Rightarrow$ $a^{m+2}\ b^{m+2}=(a^{m+1}\ b^{m+1})\ (ab)$

$\Rightarrow$ $a^{m+1}\ (a\ b^{m+1})\ b=a^{m+1}\ (b^{m+1}\ a)\ b$

$\Rightarrow$ $a\ b^{m+1}=b^{m+1}\ a$. by L and R. Cancellation Laws,

$\Rightarrow$ $a^m\ (ab^{m+1})=a^m\ (b^{m+1}\ a)$

$\Rightarrow$ $a^{m+1}\ b^{m+1}=a^m\ b^m\ ba$.

$\Rightarrow (ab)^{m+1}=a^m b^m (ba)$

$\Rightarrow (ab)^m (ab)=(ab)^m (ba)$

$\Rightarrow ab=ba \Rightarrow G$ is an abelian group.

Ex. 12. *Prove that any group of elements less than or equal to four must be abelian.*

(Allahabad 67; Delhi Hons. 69; Kanpur 69)

If the group contains only one element then that must be identity element e and it is clearly abelian.

Now let the group contain two elements one of which must be e and let the other be a then $ae=ea=a$ and hence it is abelian.

Again let e, a, b be the only three elements of the group. We shall form the composition table.

$e.e=e,\ e.a=a=a.e,\ e.b=b=b.e.$

	e	a	b
e	e	a	b
a	a	p	q
b	b	r	s

Let us fill in all the enteries written above, we have to fill in the enteries p, q, r, s. Since elements in each row or each column of the composition table should be distinct and as such p and q should be either e or b. But q cannot be b, because in that case column no. 3 will have two elements same and hence $q \neq b$ $\therefore$ $q=e$ and hence $p=b$

$\therefore$ $a.a=b,\ a.b=e$

Hence r must be equal to e as p is b, and s must be a as q is e. Therefore the composition table is as shown in next page

.	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Each row is identical with corresponding column and as such the group is abelian.

Now considcr the group of order 4 say $G=\{e, a, b, c\}$

We know that inverse of e is e and the group being of even order therefore by Q. 1 there must be an element say a which should be its own inverse *i.e* $a=a^{-1}$ and $a^2=aa^{-1}=e$ and in this case the remaining two elements b and c could be such that either $b^{-1}=b$, or $c^{-1}=c$ *i.e.* $b^2=bb^{-1}=e$, or $c^2=cc^{-1}=e$ and hence each element except the identity is of order 2 or we can say that each element is its own inverse and hence by Ex. 1. P. 84 the group is abelian.

The second possibility is that $b^{-1}=c$ and $c^{-1}=b$,

then $bc=bb^{-1}=e$, $cb=c\,c^{-1}=e$. Also $a^2=a\cdot a=e$.

Now let us form the composition table with the known data.

i.e. $e.\ e=e$, $e\cdot a=a$, $e\cdot b=b$, $e\cdot c=c$; $a\cdot e=a$, $a.a=e$;

$b.e=b$, $b.c=e$; $c.e=c$, $c.b=e$

.	e	a	b	c
▪	e	a	b	c
a	a	e	p	q
b	b	r	s	e
▪	c	t	e	u

We have to find out the unknown elements p, q, r, s, t, u.

Keep in view that each row or each column should contain four distinct elements.

Now $a.b=b$ or c, but if $a.b=b$ it would mean that $a=e$ which is not true hence $a.b=c$ so that $p=c$ and hence $q=b$

Now $b.a=c$ or a but if $b.a=a$ then $b=e$ which is not true and hence $b.a=c$ so that $r=c$ and hence $s=a$.

Therefore $t=b$ as second column should have all the elements distinct and $u=a$ as the fourth row should have all the elements distinct.

Therefore the composition table now is as shown below

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Since each row is identical with the corresponding column hence the composition is commutative.

§ 14. General law of commutativity of the elements of a group. **(Punjab 70; Meerut 70)**

If in any group G, $a_1, a_2, \ldots \ldots, a_n$ is any system of n elements commutative in pairs and

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix}$$

is any permutation of the set of n objects then

$$a_1 a_2 a_3 \ldots a_n = a_{i_1} a_{i_2} a_{i_3} \cdots a_{i_n}$$

The proof of above will be given by induction method. The given theorem holds good for $n=2$ as $a_1a_2=a_2a_1$ (elements commutative in pairs). Suppose the theorem holds

good for the products of $n-1$ or less elements. Then the following two cases arise.

Case. I. If $i_n=n$ then

$a_1 a_2 \dots a_n=(a_1 a_2 \dots a_{n-1})\, a_n$ by associative property

$=(a_{i_1} a_{i_2} \dots a_{i_{n-1}})\, a_{i_n}$ $\quad\therefore\quad n=i_n$

and also because by assumption the law holds good for $n-1$ or less elements.

$=a_{i_1} a_{i_2} \dots a_{i_{n-1}}\, a_{i_n}$ by associative law.

Case II. If $i_n=k$ where $k<n$ then

$a_1 a_2 \dots a_{k-1} a_k a_{k+1} \dots a_n$

$=(a_1 a_2 \dots a_{k-1})\,(a_k a_{k+1} \dots a_n)$

$=(a_1 a_2 \dots a_{k-1})\, a_k\, (a_{k+1} \dots a_n)$ Associative

$=(a_1 a_2 \dots a_{k-1})\,(a_{k+1} \dots a_n)\, a_k$ by assumption

$=[(a_1 a_2 \dots a_{k-1})\,(a_{k+1} \dots a_n)]\, a_k$

$=(a_1 a_2 \dots a_{k-1} a_{k+1} \dots a_n)\, a_k$

$=(a_{i_1} a_{i_2} \dots a_{i_{n-1}})\, a_{i_n}$

$=a_{i_1} a_{i_2} \dots a_{i_n}$

Hence the theorem is true by induction.

§ 15. One-one-onto mapping preserving group compositions

Introduction.

Let G and G' be two groups and f be a mapping $f : G \to G'$.

One one mapping.

The mapping f is said to be one-one if different elements of G have different f images in G'

i.e. $\quad f(x)\neq f(y) \Rightarrow x\neq y$

or $\quad f(x)=f(y) \Rightarrow x=y$.

Onto mapping.

The mapping f is said to be onto if every element of G' is the f image of certain element of G. In other words if corres-

ponding to every element a' of G' $\exists$ an element $a \in G$ such that $f(a)=a'$.

Mapping preserving group composition.

We shall illustrate this by the following example.

Let $G=(I, +)$ *i.e.* the set of all integers with additive composition *i e.* $G=\{\ldots -3, -2, -1, 0, 1, 2, 3\ldots\}$ and $G'=\{2^a : a=0, \pm 1, \pm 2, \pm 3 \ldots\}$ with multiplication composition.

Let f be a mapping from G to G' *i.e.* $f: G \to G'$ defined by $f(a)=2^a \ \forall\ a \in G$.

f is one-one $f(a)=f(b) \Rightarrow 2^a=2^b \Rightarrow a=b$

f is onto. Let $y \in G' \Rightarrow y=2^a=f(a)$ where $a \in G$

Thus for each element y in $G' \exists$ an element $a \in G$ s.t. $y=f(a)$

Hence f is onto.

Again $a+b \in G$ and $f(a)=2^a$ and $f(b)=2^b$ by definition of f.

$\therefore\ f(a+b)=2^{a+b}$ by def. $=2^a.2^b=f(a).f(b)$

i.e. f-image of the sum of two elements of G goes to the product of their f images in G'. *i.e.* the mapping f preserves the compositions in the two groups which are addition and multiplication.

Here the two groups were having different compositions. They may have the same compositions as well.

i.e. if we choose $G'=\{ma : a=0, \pm 1, \pm 2, \pm 3\ldots\}$ with additive composition.

$f: G \to G'$ defined by $f(a)=ma \ \forall\ a \in G$.

then f is clearly one-one and onto mapping.

Now $a+b \in G$ and $f(a)=ma$ and $f(b)=mb$.

$\therefore\ f(a+b)=m(a+b)=ma+mb$ by distributive law

$=f(a)+f(b)$

i.e. the image of sum of two elements of G is sum of the images of the two elements *i.e.* mapping f preserves the

compositions in the two groups which are both additive groups.

§ 16. Isomorphism of groups.

(Allahabad 68; Meerut 68, 69; Lucknow 68,69; B.H.U. 70)

Definitions. *Let G and G' be two groups with binary compositions denoted as o and o' respectively. If there exists a one-one mapping f of G onto G' such that*

$$f(a \circ b) = f(a) \circ' f(b) \quad \forall\ a, b \in G. \qquad \ldots(1)$$

then we say that the group G is isomorphic to group G' and is denoted as $G \cong G'$.

The mapping f is said to be an isomorphic mapping or simply an isomorphism of G onto G'. **(Meerut 68)**

We may as usual write the condition (1) by using simply the multiplicative notation as

$$f(ab) = f(a)\, f(b). \qquad \ldots(2)$$

The condition (1) emphasizes that the mapping f preserves the group compositions.

In multiplicative notation it says that image of poduct = product of images and in additive notation it says that image of sum = sum of images.

Let $a, b, c \in G$ and their corresponding images in G' be a', b', c' *i.e.* $f(a) = a', f(b) = b', f(c) = c'$.

Now if $ab = c$ then $f(ab) = f(c)$

or $f(a)\, f(b) = f(c)$ by (2) or $a'b' = c'$

i e. each relation between elements of G is carried over to a similar relation between elements of G'.

Isomorphism. *A one-one onto mapping preserving group composition is called an isomorphism.*

Note. If $G \cong G'$ then there may exist more than one isomorphism of G onto G'. Further if G is a finite group then

G' should also be finite having the same number of elements as in G otherwise the mapping $f : G \to G'$ will not be one-one and onto.

Exercise 5

1. $G=(I, +)$

$G'=\{2^a : a \in I\}$ *with multiplicative composition.*

We have already shown on P 93 that the mapping $f.G \to G'$ defined by $f(a)=2^a$ is one-one-onto and preserves group composition and hence G is isomorphic to G' *i.e.* $G \cong G'$

2. $G=(I, +)$

$G'=(na : a \in I)$ *with additive composition.*

We have already shown on P. 93 that $G \cong G'$.

3, $G=\{$*set* R^+ *of* $+$*ive real numbers*$\}$ *with multiplication as its comosition.*

$G'=\{$*set* R *of real numbers*$\}$ *with additive composition*

$f : G \to G'$ *defined by* $f(x)=\log x. \quad x \in G.$

To show that f *is an isomorphism and hence* $G \cong G'$.

In order to show that f is an isomorphism we have to show that f is one-one onto and preserves group compositions.

f is one-one

Let $x, y \in G$ *i. e.* R^+ then

$$f(x)=f(y) \Rightarrow \log x=\log y \Rightarrow x=y$$

and hence f is one-one mapping.

f is onto

For onto we have to show that each element belonging to G' *i.e.* R is the f image of some element $\in G$ *i.e.* R^+.

Let $z \in G'$ and we will show that it is the f image of some $+$ive real number belonging to G. Now e^x is a $+$ive real number and as such $\in G$

$\therefore$ $f(e^z) = \log(e^z)$ by definition of f

$= z$.

Thus $z \in G$ is the f image of $e^z \in G$. Hence the mapping is onto.

Again let $x, y \in G$ so that $xy \in G$.

Also $f(x) = \log x$ and $f(y) = \log y$

$f(xy) = \log(xy) = \log x + \log y = f(x) + f(y)$.

Thus the mapping f preserves the group compositions. Hence it is an isomorphism and the two groups are isomorphic *i.e.* $G \cong G'$

Ex. 4. *G = {set R of real numberss} with additive composition.*

G = {set R^+ of +ive real numbers} with multiplicative composition.

Show that $f: G \to G'$ defined by $f(x) = e^x$, $x \in G$ is an isomorphism **(Gujarat M. Sc. 70; Delhi 70; Meerut 68, 69)**

The mapping f is one-one because

$$f(x) = f(y) \Rightarrow e^x = e^y \Rightarrow x = y$$

Also f is onto also because corresponding to each +ive real number $z \in G'$ there exists a real number $\log z \in G$ such that

$f(\log z) = e^{\log z} = z$.

Thus $z \in G'$ is the f image of some real number $\log z \in G$. Hence the mapping is onto.

Again let $x, y \in G$ so that $x + y \in G$.

Also $f(x) = e^x$ and $f(y) = e^y$.

$\therefore$ $f(x+y) = e^{x+y} = e^x . e^y = f(x) f(y)$.

Thus the mapping f preserves the group compositions. Hence f is an isomorphism and the two groups are isomorphic *i.e.*, $G \cong G'$.

Ex. 5. *Prove that the set of all complex numbers under*

addition is a group which is isomorphic to itself under the identity mapping as well as under the mapping which takes every number into its conjugate.

Let $f : C \to C : f(z) = z \ \forall \ z \in C$

i e., f is an identity mapping which is clearly one-one and onto.

Again $f(z_1+z_2)=z_1+z_2=f(z_1)+f(z_2)$ by def. of f.

Hence the mapping f preserves group composition and hence is an isomorphism from C to C. $\therefore \quad C \cong C$.

Let $g : C \to C : f(z)=\bar{z} \ \forall \ z \in C$

If $z_1=x_1+iy_1$, $z_2=x_2+iy_2 \in C$ then

$g(z_1)=g(z_2) \Rightarrow \bar{z}_1=\bar{z}_2 \Rightarrow x_1-iy_1=x_2-iy_2 \Rightarrow x_1=x_2$

and $y_1=y_2 \Rightarrow z_1=z_2$.

Hence g is one-one. It is also onto.

Again $g(z_1+z_2)=\overline{(z_1+z_2)}=\bar{z}_1+\bar{z}_2=g(z_1)+g(z_2)$ by def. of g.

Thus the mapping g preserves group compositions and hence is an isomorphism from C to C, $\therefore \quad C \cong C$.

6. *Prove that the group*;

$G=\{1, -1, i, -i\}$ *with multiplicative composition is isomorphic to the group.*

$G_1=\{0, 1, 2, 3\}$ *with addition modulo 4 as composition.*

(Raj. M. Sc. 69)

It should be understood that only elements of equal order can be mapped on each other through an isomorphic mapping.

Here the orders of elements $1, -1, i, -i$ are respectively,

$1, 2, 4, 4 \qquad [a^n=e]$

whereas the orders of 0, 1, 2, 3 of G' under addition modulo 4 composition are 1, 4, 2, 4.

Hence we define a mapping $f : G \to G'$ such that

$f(1)=0, f(-1)=2, f(i)=1, f(-i)=3$.

Clearly the mapping is one-one and onto.

Again $(i)\,(-i)=-i^2=1.$

$\therefore\ f(i.-i)=f(1)=0=1+3=f(i)+f(-i)$

$+4$

i.e., $f(xy)=f(x)+f(y).$

Thus the mapping f preserves group composition and hence it is an isomorphism and therefore $G\cong G'$.

Note :—We could define the mapping f as under also

$f(1)=0, f(-1)=2, f(i)=3, f(-i)=1$

and arguing as above we can show that f is an isomorphism.

7. *If* $G=\{1, -1, i, -i\}$ *with multiplication as composition*

$G'=\{$*set of residue classes mod 4*$\}$

composition as addition of residue classes.

show that ; G is isomorphic to G'.

$G'=\{\{0\}, \{1\}, \{2\}, \{3\}\}$.

$\{0\}$=set of all those integers which are congruent to 0 modulo 4

i.e. $x-0=4k\ \forall\ k\in I\ \therefore\ \{0\}=\ldots-12, -8, -4, 0\ 4, 8, 12\ldots$

$\{1\}$=set of all those Integers which are congruent to 1 modulo 4 *i.e.*, $x-1=4k\ \forall\ k\in I$

i.e., all those numbers which when divided by 4 leave a remainder 1,

$\therefore\ \{1\}=\ldots-11, -7, -3, 1, 5, 9, 13\ldots\ldots$

Similarly $\{2\}=\ldots\ldots-10, -6, -2, 2, 6, 10, 14\ldots\ldots$

$\{3\}=\ldots\ldots-9, -5, -1, 3, 7, 11, 15\ldots\ldots$

Also $\{r_1\}+\{r_2\}=\left\{\begin{matrix}r_1+r_2\\ +4\end{matrix}\right\}$

$\therefore\quad \{2\}+\{3\}=\left\{\begin{matrix}2+3\\ +4\end{matrix}\right\}=\{1\}$

$\{1\}+\{3\}=\left\{\begin{matrix}1+3\\ +4\end{matrix}\right\}=\{0\}$ etc.

Just as in last example we define a mapping f as under keeping in view that elements of equal order can be mapped on to each other through an isomorphism

$f(1)=\{0\}, f(-1)=\{2\}, f(i)=\{1\}, f(-i)=\{3\}$

The above mapping is evidently one-one onto.

Again $i.-i=-i^2=1$

$\therefore \quad f(i.-i)=f(1)=\{0\}=\{1\}+\{3\}=f(i)+f(-i)$

i.e., $f(xy)=f(x)+f(y)$ *i.e.*, the mapping preserves the group compositions and hence it is an isomorphism. Therefore $G\cong G'$.

8. *Prove that the multiplicative group G consisting of three cube roots of unity i.e., 1, w, w^2 is isomorphic to group G′ of residue classes mod (3) under addition of residue classes.*

Define a mapping $f: G \to G'$ such that

$f(1)=\{0\}, f(w)=\{1\}, f(w^2)=\{2\}$ etc.

9. *Show that the group :*

$G=\{0, 1, 2, 3\}$ *Addition modulo 4.*

is isomorphic to the group.

$G'=\{1, 2, 3, 4\}$ *multiplication modulo* 5.

order of 1 in G is 4 $\quad\therefore\quad 1+1+1+1=\underset{+4}{4}=0=$ identity

order of 2 in G' is 4 $\quad\therefore\quad 2.2.2.2=\underset{\times 5}{16}=1=$ identity

order of 2 in G is 2 $\quad\because\quad 2+2=\underset{+4}{4}=0$

order of 4 in G' is 2 $\quad\because\quad 4\times 4=\underset{\times 5}{16}=1$

order of 3 in G is 4 $\quad\because\quad 3+3+3+3=\underset{+4}{12}=0.$

order of 3 in G' is 4 $\quad\because\quad 3\times\ \times 3\times 3=\underset{\times 5}{81}=1$

Hence we define a mapping $f: G \to G'$ such that

$f(0)=1, f(1)=2, f(2)=4, f(3)=3.$

This is done so as we know that the elements of same order are mapped on to each other through an isomorphism. The mapping is clearly one-one onto.

$$2+3=\underset{+6}{5}=1$$

$$\therefore \quad f(2+3)=f(\underset{+6}{5})=f(1)=2=\underset{\times 5}{4.3}=f(2).f(3)$$

i.e, $f(x+y)=f(x).f(y).$ (+6, ×5)

i.e., the mapping preserves the group compositions. $\therefore G \cong G'$

Note. We could also define the mapping f as under keeping in mind that elements of same order are mapped on to each other.

$$f(0)=1, f(1)=3, f(2)=4, f(3)=2,$$

Here $f(2+3)=f(\underset{+4}{5})=f(1)=3=\underset{\times 5}{4.2}=f(2).f(3)$

i.e., $f(x+y)=f(x).f(y).$ (+4, ×5)

10. *Show that the multiplicative group*

$$[I, -I, i, -i]$$

is isomorphic to permutation group.

$\{I, (a\ \ b\ \ c\ \ d),\ (ac)\ (bd),\ (a\ \ d\ \ c\ \ b)\}$

on symbols a, b, c, d with product of permutations as group composition. **(B. H. U. 70)**

The order of elements in the first group are as under

$o(1)=1, o(-1)=2, o(i)=4, o(-i)=4.$

Clearly order of $I=1$ so we define f such that $f(1)=I$...1

Again $(a\ \ b\ \ c\ \ d)=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$

$$\therefore\ (a\ \ b\ \ c\ \ d)^2=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ b & \blacksquare & d & a \end{pmatrix}\begin{pmatrix} b & c & d & \blacksquare \\ c & d & a & b \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}$$

$$\therefore\ (a\ \ b\ \ c\ \ d)^3=\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}\begin{pmatrix} a & b & c & d \\ b & c & d & \blacksquare \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}\begin{pmatrix} c & d & \blacksquare & b \\ d & a & b & c \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}$$

$$\therefore\ (a\ \ b\ \ c\ \ d)^4=\begin{pmatrix} a & b & c & d \\ d & \blacksquare & b & c \end{pmatrix}\begin{pmatrix} a & b & \blacksquare & d \\ b & c & d & a \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}\begin{pmatrix} d & a & b & c \\ a & b & c & d \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}=I$$

$\therefore$ order of $(a\ \ b\ \ c\ \ d)$ is 4, so we define that

$$f(I)=(a\ \ b\ \ c\ \ d) \qquad \text{.. (2)}$$

Again $(ac)\ (bd)=\begin{pmatrix} a & c & b & d \\ c & a & d & b \end{pmatrix}=\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}$

$$\therefore\ [(ac)\ (bd)]^2=\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ c & d & \blacksquare & b \end{pmatrix}\begin{pmatrix} c & d & a & b \\ a & b & c & d \end{pmatrix}$$
$$=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}=I$$

$\therefore$ order of $(ac)\,(bd)$ is 2 and so we define that

$$f(-1)=(ac)\,(bd). \qquad \ldots(3)$$

It can be verified that order of $(a \quad d \quad c \quad b)$ is 4.

so that $$f(-i)=(a \quad d \quad c \quad b) \qquad \ldots(4)$$

Hence $f: G \to G'$ such that

$$f(1)=I=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

$$f(i)=(a \quad b \quad c \quad d)=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix}$$

$$f(-1)=(ac)\,(bd)=\begin{pmatrix} a & c & b & d \\ c & a & d & b \end{pmatrix}$$

$$f(-i)=(a \quad d \quad c \quad b)=\begin{pmatrix} a & d & c & b \\ d & c & b & a \end{pmatrix}$$

Evidently the mapping is one-one onto :

Again $$i.-i=-i^2=1.$$

$$\therefore \quad f(i.-i)=f(1)=I=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}$$

Again $$f(i).f(-i)=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} o \begin{pmatrix} a & d & c & b \\ d & c & b & a \end{pmatrix}$$

$$=\begin{pmatrix} a & b & c & d \\ b & c & d & a \end{pmatrix} o \begin{pmatrix} b & c & d & a \\ a & b & c & d \end{pmatrix}$$

$$=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}=I=f(i.-i)$$

Thus $f(xy)=f(x)\,f(y)$ and hence it preserves group compositions. Hence $G \cong G'$

you can choose any two elements of G and show that $f(x.y)=f(x).f(y)$.

11. *Show that the permutation group*

$G=\{I, (a \quad b \quad c \quad d), (ac).(bd), (a \quad d \quad c \quad b)\}$

with multiplication of permutation as the composition is isomorphic to the group.

$G'=\{1, 3, 7, 9\}$ *with multiplications modulo 10 as composition.*

As shown in last example the orders of the various permutations are 1, 4, 2, 4.

Again order of elements in the second group are as under.

$o(1)=1$, $o(3)$ is 4 because $3^4=81=1$ (mod 10)

$o(7)=4 \because 7^4=1$ under multiplication modulo 10

$o(9)=2 \because 9^2=81=1$ under multiplication modulo 10.

Keeping in mind that elements of the same order are mapped on to each other through an isomorphism we define a mapping $f: G \to G'$ such that

$f(I)=1, f[(a\ b\ c\ d)]=3, f[(ac).(bd)]=9$

$f[(a\ d\ c\ b)]=7.$

Now $(a\ b\ c\ d)\ o\ [(ac)\ o\ (bd)]$

$$=\begin{pmatrix}a & b & c & d\\ b & c & d & a\end{pmatrix} o \begin{pmatrix}a & c & b & d\\ c & a & d & b\end{pmatrix}$$

$$=\begin{pmatrix}\blacksquare & b & c & d\\ b & c & d & a\end{pmatrix} o \begin{pmatrix}b & c & d & a\\ d & \blacksquare & b & c\end{pmatrix}$$

$$=\begin{pmatrix}a & b & c & d\\ d & a & b & c\end{pmatrix}=\begin{pmatrix}a & d & c & b\\ d & c & b & a\end{pmatrix}$$

$=(a\ d\ c\ b).$

$\therefore\ f[(a\ b\ c\ d).\{(ac).(bd)\}]$

$=f(a\ d\ c\ b)=7.$

Also $f(a\ b\ c\ d).f\{(ac).(bd)\}=3\cdot 9=7$ (mod 10)

$\therefore\ f(xy)=f(x).f(y)$. Hence the mapping preserves group compositions

$\therefore\quad G\cong G'.$

Also $o(I)=1$, $o(a\ b\ c)=3$, $o(a, c, b)=3$

12. *Prove that the group*

$G=\{I, \omega, \omega^2\}$ *under multiplicative composition is isomorphic to the permutation group.*

$G'=\{I, (a\ b\ c), (a\ c\ b)\}$ *under multiplication of permutation as the composition.*

$o(1)=1$, $o(\omega)=3$, $o(\omega^2)=3$

Define $f: G \to G'$ such that

$f(1)=I, f(\omega)=(a\ b\ c), f(\omega^2=(a\ c\ b)$.

13. *If* $G=\{0, 1, 2, 3, 4\}_{+6}$

and G' *is the cyclic group* $\{a, a^2, a^3, a^4, a^5=e\}$

Show that the mapping $f: G \to G'$ *such that* $f(n)=a^n \forall n \in G$ *is an isomorphism of* G *onto* G'.

$$f(3+4)=f(2)=a^2.$$

$f(3).f(4)=a^3.a^4=a^7=a^5\cdot a^2=a^2$ $\because$ $a^5=e$

$\therefore$ $f(x+y)=f(x).f(y)$ etc.

14. *Prove that the following groups are isomorphic*

$G=[\{z : z^6=1, z \in C\}, \cdot]$

$G'=[\{0, 1, 2, 3, 4, 5\}, +6]$

The elements of G are given by

$$z=(1)^{1/6}=(\cos 2n\pi+i \sin 2n\pi)^{1/6}$$

or $$z=\left(\cos \frac{2n\pi}{6}+i \sin \frac{2n\pi}{6}\right)=e^{4n\pi/3}$$

where $n=0, 1; 2, 3, 4, 5$

$\therefore$ $z^1=e^0=1$, $z_2=e^{\pi i/3}$, $z_3=e^{2\pi i/3}$, $z_4=e^{\pi i}=-1$,

$z_5=e^{4\pi i/3}$, $z_6=e^{5\pi i/3}$

Now we shall find the order of the various elements in the two groups.

For group G .

$o(z_1)=1$, $o(z_2)=6$ $\because$ $z_2^6=e^{2\pi i}=1=$Identity

$o(z_3)=3$, $o(z_4)=2$, $o(z^5)=3$, $o(z_6)=6$

For group G′.

Order of element in group G' the composition being

addition modulo 6.

$o(0)=1,\ o(1)=6 \quad \because \quad 6(1)=\underset{+6}{6}=0=$identity

$o(2)=3,\ o(3)=2,\ o(4)=3,\ o(5)=6.$

Keeping in view that elements of same order are mapped on to each other through an isomorphism, we define a mapping $f: G \to G'$ as under.

$f(z_1)=0,\ f(z_2)=1,\ f(z_3)=2,\ f(z_4)=3,\ f(z_5)=4,\ f(z_6)=5.$

The mapping is clearly one-one onto.

Now we shall verify whether this mapping preserves group compositions or not.

Let us choose any two element say z_2 and z_5.

Then $z_2.z_5=e^{\pi i/3}.e^{4\pi i/3}=e^{5\pi i/3}=z_6.$

$f(z_2.z_5)=f(z_6)=5=1+4=f(z_2)+f(z_5).$

Hence f preserves group compositions which therefore is an isomorphism $\therefore \quad G \cong G'.$

15. *Prove that the group* $G=\{f_1, f_2, f_3, f_4\}$ *composite compositions where*

$f_1(z)=z,\ f_2(z)=-z,\ f_3(z)=1/z, f_4(z)=-1/z,$

is isomorphic to the group

$$G'=\{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

where σ_i*'s are the permutations*

$\sigma_1=I,\ \sigma_2=(ab),\ \sigma_3=(cd),\ \sigma_4=(ab)\ (cd).$

In group G, f_1 is the identity transformation and its order is 1.

Also $f_2^2(z)=f_2 f_2(z)=f_2(-z)=z=z=f_1(z)$

$\therefore \quad f_2^2=f_1=$identity.

Hence order of $f_2=2$. Similarly we can show that the orders of f_3 and f_4 are each two.

Again in G', σ_1 is the identity permutation and its order is 1.

We may verify that order of each of the remaining permutations is 2.

We know that elements of same order are mapped on to each other through an isomorphism and as such we define a mapping. $\phi : G \to G'$

such that $\phi(f_1)=\sigma_1$, $\phi(f_2)=\sigma_2$, $\phi(f_3)=\sigma_3$, $\phi(f_4)=\sigma_4$.

This mapping is clearly one-one onto. Let us verify if it preserves group composition or not.

$f_2 f_3(z)=f_2(1/z)=-1/z=f_4(z)$ $\quad\therefore\quad f_2 f_3=f_4$.

$\phi(f_2 f_3)=\phi(f_4)=\sigma_4=(ab)(cd)=\sigma_2\sigma_3=\phi(f_2)\cdot\phi(f_3)$.

Hence group compositions are preserved.

Note. If we form the composition table for the two groups as under

For G					For G′				
I	f_1	f_2	f_3	f_4	σ	σ_1	σ_2	σ_3	σ_4
f_1	f_1	f_2	f_3	f_4	σ_1	σ_1	σ_2	σ_3	σ_4
f_2	f_2	f_1	f_4	f_3	σ_2	σ_2	σ_1	σ_4	σ_3
f_3	f_3	f_4	f_1	f_2	σ_3	σ_3	σ_4	σ_1	σ_2
f_4	f_4	f_3	f_2	f_1	σ_4	σ_4	σ_3	σ_2	σ_1

We observe from above that if we replace f_1, f_2, f_3, f_4 in the table for G by $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ respectively we get the complete composition table for G'.

i.e. $\phi[f_3 f_4]=\phi(f_2)=\sigma_2=\sigma_3\ \sigma_4=\phi(f_3)\,\phi(f_4)$

Hence the mapping ϕ preserves the group composition in G and G'.

16 *Prove that every group of order 2 is isomorphic to every other group of order 2. In other words abstractly speaking, there exists only one group of order 2. Prove the same result for groups of order 3.*

$G=\{(a, b), o\}$

Since G is a group, one of the elements say a must be identity. Hence we have the following composition table for the operator o. Keep in mind that in the composition table for a group, each element of the groupoccurs only once in any row or column. Also $p\ o\ e=e\ o\ p=p\ \forall\ p \in G$.

o	a	b
a	a	b
b	b	$\times$

o	a	b
a	a	b
b	b	a

We have filled in three places because a is identity. The fourth place is filled by keeping in mind the observation made above.

Now consider two groups.
$(G_1, o_1)=\{(a_1, b_1), o_1\}$, $(G_2, o_2)=\{(a_2, b_2), o_2\}$
We have the following composition tables.

o_1	a_1	b_1
a_1	a_1	b_1
b_1	b_1	a_1

o_2	a_2	b_2
a_2	a_2	b_2
b_2	b_2	a_2

If we define $f : G_1 \to G_2$ such that

$$f(a_1)=a_2 \qquad f(b_1)=b_2$$

Then clearly f is one-one onto.

Also $f(a_1\ o_1\ b_1)=f(b_1)=b_2=a_2\ o_2\ b_2=f(a_1)\ o_2\ f(b_1)$

Thus the mapping f preserves the group compositions and hence f is an isomorphis *i.e.* $G_1 \cong G_2$.

Composition table for $G=\{(a, b, c), o\}$ where a is identity.

o	a	b	c
a	a	b	c
b	b	P	Q
c	c	R	S

Now $b\ o\ b \neq b$ as b already occurs in 2nd row.

Also $b\ o\ b \neq a$ because then as $b\ o\ c$ will be c which will not be possible as c already occurs in 3rd column.

$\therefore$ $b\ o\ b=c$ $\therefore$ $P=c$ and naturally $b\ o\ c=a=Q$

Having found $P=c$ we can say $R=a$ from column 2 and as $Q=a$ we can say $S=b$ from column no. 3

o	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

Rest is as above.

§ 17. Important properties of isomorphic mappings.

If the mapping $f : G \to G'$ is isomorphic then

(*i*) *Identities correspond i.e., if e is the identity of G then $f(e)=e'$ is identity of G' i.e., image of the identity of G is the identity of G'.*

(Meerut M. Sc. 67; Alld. 65, 68, 70; B, H. U. 65; Kanpur 70: Luck. 68)

(*ii*) *Inverses correspond i.e., the image of the inverse of an element of G is the inverse of the image of that element i.e.,* $f(a^{-1})=[f(a)]^{-1}$.

(Kanpur 70; B. H. U. 65; Luck. 68; Meerut M. Sc. 68; Alld. 65; 68, 70)

(*iii*) *The order of an element and its image are the same i e.* $o(a)=o[f(a)]$.

Proof. Since f is one-one onto mapping therefore corresponding to any element $a' \in G'$ ∃ an element $a \in G$ such that $f(a)=a'$.

If e be the identity of G then $f(e)=e'$ say G'. We shall show that e' is the identity of G'.

Now $ae=a$ because e is identity of G

$\therefore \quad f(ae)=f(a)$

or $\quad f(a)\,f(e)=f(a) \quad \because$ f is an isomorphic mapping

or $\quad a'\,e'=a' \quad \ldots(1)$

Similarly $ea=a \quad \therefore \quad f(ea)=f(a)$

or $\quad f(e)\,f(a)=f(a) \quad$ or $\quad e'\,.\,a'=a' \quad \ldots(2)$

Hence from (1) and 2, we get

$$a'\,e'=e'\,a'=e' \quad \forall\ a' \in G'$$

Hence by definition e' is identity of G'

But $e'=f(e)=$identity of G'

or Image of the identity of G=identity of G'

(*ii*) Let $a \in G$ and a^{-1} be the inverse of a, so that $a\,a^{-1}=e$ and $a^{-1}\,a=e \ \forall\ a \in G$.

$\therefore \quad f(a\,a^{-1})=f(e) \quad$ or $\quad f(a)\,f(a^{-1})=e' \quad$ where e' is identity of G'.

Also $\quad f(a^{-1}\,a)=f(e) \quad$ or $\quad f(a^{-1})\,f(a)=e'$

From above we conclude that inverse of $f(a)$ is $f(a^{-1})$

i.e., $\quad [f[a)]^{-1}=f(a^{-1})$

or image of inverse of an element of G

i.e., $f(a^{-1})$ = Inverse of the image of that element

i.e., $[f(a)]^{-1}$

(*iii*) Let n be the order of $a \in G$ so that $a^n = e$ where n is the least +ive integer satisfying this relation and we have to show that the order of its image $f(a)$ is also n

i.e. $[f(a)]^n = e'$.

Now $a^n = e \Rightarrow f(a^n) = f(e) = e'$ say where e' is the identity of G'.

or $f(a \,.\, a \,.\, a \,\ldots\, n \text{ times}) = e'$

or $f(a) \,.\, f(a) \,.\, f(a) \ldots \,.\, n \text{ times} = e'$ by def. of f

or $[f(a)]^n = e'$

Hence the order of $f(a)$ is less than or equal to n.

Let us suppose that m is the order of $f(a)$ where $m < n$ so that $[f(a)]^m = f(e)$

or $f(a) \,.f(a) \ldots\ldots m \text{ times} = f(e)$

or $f(a \,.\, a \,.\, a \,\ldots\ldots m \text{ times}) = f(e)$ by def. of f

or $f(a^m) = f(e) \Rightarrow a^m = e$

where $m < n$ but this contradicts the definition of order of a being n, where n is the least +ive integer such that $a^n = e$. Hence there can not be any other integer m less than n such than $a^m = e$.

Therefore $m = n$.

or order of $f(a)$ = order of a,

or order of the image of an element = order of that element

Theorem. 15. *The relation of isomorphism in the set of all groups is an equivalence relation.*

(Agra 70; Punjab 70; Gorakhpur 70; Luckhnow 68; Meerut B. Sc. 68. 69; M. Sc. 69)

Let $G_1, G_2, G_3, \ldots$ be the elements of the set of groups. In order to prove that the relation of isomorphism is an equivalence relation we have to show that it is reflexive, symmetric and transitive

1. Reflexive. To prove that $G_1 \cong G_1$. This is clearly true because there exists an identity mapping $I : G_1 \to G_1$ which is one-one onto and preserves group compositions and hence is an isomorphism.

2. Symmetric. If $G_1 \cong G_2$ then $G_2 \cong G_1$ *i.e.* we have to show that there exists a one-one onto mapping from G_2 to G_1 preserving group compositions.

As $G_1 \cong G_2$ therefore there exists a one-one onto mapping $f : G_1 \to G_2$. which is an isomorphism. Since f is one-one onto therefore there exists a mapping $f^{-1} : G_2 \to G_1$, which is also one-one onto.

Now we have to show that this mapping f^{-1} is an isomorphism, *i.e.* it preserves group compositions. For this we have to show that if a_2, b_2. be any elements of G_2 then

$$f^{-1}(a_2\, b_2) = f^{-1}(a_2) \,.\, f^{-1}(b_2). \qquad \ldots(1)$$

Let $f^{-1}(a_2) = a_1$ and $f^{-1}(b_2) = b_1$. where $a_2, b_2 \in G_2$ and $a_1, b_1 \in G_1$.

$\therefore$ $f(a_1) = a_2$ and $f(b_1) = b_2$.

$$\text{Now } f^{-1}(a_2\, b_2) = f^{-1}[f(a_1)\, f(b_1)] \qquad \ldots(2)$$

$$= f^{-1}[f(a_1\, b_1)]$$

$\because$ f is an isomorphic mapping

$$= a_1\, b_1 = f^{-1}(a_2) \,.\, f^{-1}(b_2).$$

Hence we prove the relation (1) showing thereby that f^{-1} is an isomorphic mapping from G_2 to G_1.

3. Transitive. Let G_1, G_2, G_3 be any three groups such that $G_1 \cong G_3$, *i.e.* there exists an isomorphic mapping

$$f : G_1 \to G_2$$

and $G_2 \cong G_3$, *i.e.* there exists an isomorphic mapping

$$g : G_2 \to G_3.$$

To show that $G_1 \cong G_3$ *i.e.* there exists an isomorphic mapping from G_1 to G_3.

Since both f and g are one-one onto mappings therefore the resultant mapping $g f$ is also one-one onto *i.e.*

$$g f : G_1 \to G_3.$$

In order to show that $g f$ is an isomorphic mapping we have to establish that

$$(g f)(a b) = (g f) a \,.\, (g f)\, b \qquad \ldots(1)$$
$$a, b \in G_1$$

Now $(g f)(a b) = g[f(a b)] = g[f(a) \,.\, f(b)]$

$\therefore$ f is an isomorphism

$= g[f(a)] \,.\, g[f(b)]$

$\because$ g is an isomorphism

$= (g f) a \,.\, (g f) b.$

Thus the relation (1) is proved and as such the resultant mapping $g f$ is also an isomorphic mapping.

$$\therefore \quad G_1 \cong G_3.$$

$$\therefore \quad G_1 \cong G_2 \text{ and } G_2 \cong G_3 \Rightarrow G_1 \cong G_3$$

Hence the relation of isomorphism in the set of all groups is an equivalence relation.

Note. We can now say that the set of all groups is partitioned into mutually disjoint classes, such that any two groups belonging to the same class are isomorphic to each other whereas the groups belonging to different classes are not isomorphic.

In an equivalence classes, one member of a class characterises the whole class so far as the group properties are concerned. It mear s that by studying the properties of a single group of one class the propert es of all the groups of that class can be determined.

§ 18. Transference of group structures.

Theorem 16. *If G is a group and G' is a set with a composition denoted multiplicatively and there exists a one-one mapping of G onto G' such that*

$$f(a\ b)=f(a)\ .\ f(b),\ \forall\ a, b \in G,$$

then G' is also a group isomorphic to G.

In order to prove that G' is also a group we have to establish the postulates of a group, *i.e.* associative, Identity and inverse for the given composition in G'.

Let a', b', c' be any three elements of G', so that

$$f(a)=a', f(b)=b', f(c)=c',$$

where $a, b, c \in G$ because f is one-one onto mapping from G to G'.

Associative. We have to establish that

$$(a'\ b')\ c'=a'\ (b'\ c').$$

Now $(a'\ b')\ c'=[f(a)\ .\ f(b)]\ f(c)=[f(a\ b)]\ f(c)$
by given condition

$=f[(a\ b)\ c]=f[a\ (b\ c)]$
$\because$ G is a group. $\therefore$ $(a\ b)\ c=a\ (b\ c)$

$=f(a)\ .\ [f(b\ c)]=f(a)\ [f(b)\ .\ f(c)]$

$=a'\ (b'\ c').$

Hence the relation (1) is proved.

Identity. Let e be the identity of G, so that

$$a\ e=e\ a=a\ \forall\ a \in G.$$

Consider $[f(e)]\ a'=f(e)\ .\ f(a)=f(e\ a)$ by def. of f

$=f(a)=a'$ $\because$ $e\ a=a.$

Similarly $a'\ .\ [f(e)]=f(a)\ .\ f(e)=f(a\ e)=f(a)=a'.$

Hence $[f(e)]\ a'=a'\ [f(e)]=a'$

$\therefore$ $f(e)$ is the identity of G' and this $f(e)$ is the image of the identity of G.

Inverse. S nce G is a group we have

$$a\ a^{-1}=a^{-1}\ a=e\ \forall\ a \in G.$$

$\therefore$ $f(a\ a^{-1})=f(e)$ or $f(a).f(a^{-1})=f(e)$

or $a'\ f(a^{-1})=f(e)=$identity of G' ...(2)

Similarly $a^{-1}a=e \therefore f(a^{-1}a)=f(e)$

or $f(a^{-1})\,f(a)=f(e)$

or $f(a^{-1})\,a'=f(e)=$identity of G' ...(3)

Relations (2) and (3) show that the inverse of $a' \in G'$ is $f(a^{-1})$, *i e.* $(a')^{-1}=f(a^{-1})$.

or $[f(a)]^{-1}=f(a^{-1})$.

Hence all the group postulates are satisfied showing there by that G' is a group and it will be isomorphic to G because G is isomorphic to G' under given conditions and the relation of isomorphism is an equivalence relation and as such symmetric property is satisfied.

Theorem 17.

Cayley's Theorem. *Every finite group G is isomorphic to a permutation group.*

(Utkal 70; Rai. M.Sc. 67; Allahabad 64; Meerut B-Sc. 68, 69; Kanpur 69; B.H.U. 70, 67, 62; Lucknow 70; Aligarh 65; Delhi Hons 69; Punjab 69)

Let G be a finite group of order n, *i.e.*

$$G=\{a_1, a_2, a_3, \ldots\ldots a_n\}.$$

We shall form the n permutations as under. Let $b \in G$ be any of the n elements of G, then the products

$$a_1b,\ a_2b,\ a_3b,\ \ldots,\ a_nb$$

will all be distinct and shall be elements of G which is a group For if not let any two of the products say

$$a_ib=a_jb,$$

then by cancellation law it implies that $a_i=a_j$ which contradicts the fact that the group G is of order n. Hence we conclude that $a_1b, a_2b, \ldots\ldots a_nb$ are again the n elements of G in some order, where b is one of these a^s.

Therefore $a_i \to a_ib$ is one-one correspondence of G onto to itself and hence

$$\begin{pmatrix} a_1 & a_2 \ldots a_n \\ a_1 b & a_2 b \ldots a_n b \end{pmatrix}$$

is a permutation on n symbols.

For convenience sake we denote this permutation as

$$\begin{pmatrix} a_i \\ a_i b \end{pmatrix} \quad \text{or} \quad \pi_b,$$

where b is any of the n elements of G. In this way we shall get n permutations like π_b for n different values of b. Let G' be the set of these n permutations,

i.e. $$G' = [\pi_b : b \in G].$$

Let us now first establish that G' is a group.

Closure property. Let π_a and π_b be any two elements of G' then for each $a_i \in G$

we have $$\pi_a \pi_b (a_i) = \pi_b [\pi_a (a_i)] = \pi_b (a_i a)$$
$$= (a_i a) b = a_i (ab). \quad \because \quad G \text{ is a group.}$$

or $$\pi_a \pi_b (a_i) = \pi_{ab} (a_i) \qquad \forall \ a_i \in G$$

$\therefore$ $$\pi_a \pi_b = \pi_{ab}.$$

Since $a, b \in G$ and G is a group $\therefore$ $ab \in G$ and hence π_{ab} belongs to G'. Thus G' is closed for multiplication of permutation as the composition.

Associative. Multiplication of permutations is always associative.

Identity. Let e be the identity of G and $a \in G$

then $$\pi_a \, o \, \pi_e (a_i) = \pi_e [\pi_a (a_i)] = \pi_e (a_i a).$$
$$= (a_i a) e = a_i (a e) = a_i a$$

or $$\pi_a \, o \, \pi_e (a_i) = a_i a = \pi_a (a_i) \qquad \forall \ a_i \in G$$

$\therefore$ $$\pi_a \, o \, \pi_e = \pi_a.$$

Similarly $\pi_e \, o \, \pi_a = \pi_a$.

Hence π_e is the identity in G'

Inverse. $\pi_a \, o \, \pi_a^{-1} = \pi_{a \, a^{-1}} = \pi_e =$ identity of G'

$$\pi_a^{-1} \, o \, \pi_a = \pi_a^{-1} a = \pi_e = \text{identity of } G'$$

$\therefore$ π_a^{-1} is the inverse of element π_a of G'.

Hence G' is a group.

Again let us define a mapping $f : G \to G'$ such that

$$f(b) = \begin{pmatrix} a_i \\ a_i b \end{pmatrix} = \pi_b \, (b \in G).$$

This mapping is clearly one-one for

$$f(b) = f(c) \Rightarrow \pi_b = \pi_c \Rightarrow \begin{pmatrix} a_i \\ a_i b \end{pmatrix} = \begin{pmatrix} a_i \\ a_i c \end{pmatrix}$$

$$\Rightarrow a_i b = a_i c \Rightarrow b = c.$$

Also it is an onto mapping for each permutation in G' has its pre-image in G.

Now if we establish that f is an isomorphism, *i.e.*

$$f(b\,c) = f(b) \, o \, f(c),$$

then by the last theorem of transference of group structure we hall be able to say that G' is a group which is isomorphic to G.

Now $f\ (bc) = \pi_{bc} = \begin{pmatrix} a_i \\ a_i bc \end{pmatrix} = \begin{pmatrix} a_i \\ a_i b \end{pmatrix} \begin{pmatrix} a_i b \\ a_i bc \end{pmatrix}$.

Now $\begin{pmatrix} a_i b \\ a_i bc \end{pmatrix} = \begin{pmatrix} (a_i b) \\ (a_i b)\ c \end{pmatrix}$. It is the same permutation as $\begin{pmatrix} a_i \\ a_i c \end{pmatrix}$ with columns different as $a_i b$ and a_i are the same elements arranged in a different manner.

$$\therefore \quad f\ (bc) = \begin{pmatrix} a_i \\ a_i b \end{pmatrix} o \begin{pmatrix} a_i \\ a_i c \end{pmatrix} = \pi_b \, o \, \pi_c$$

$$= f(b) \, o \, f(c).$$

Hence there exists a one-one onto mapping $f : G \to G'$ such that

$$f(bc) = f(b) \, o \, f(c).$$

Therefore the set G' is a group isomorphic to G by Th. 16, P. 112.

Note. The permutation group G' to which G is isomorphic is called the **regular permutation group.**

Excercise 6

1. *Find the regular permutation group isomorphic to the multiplicative group* $\{1, \omega, \omega^2\}$.

The three permutations are obtained as under by Cayley's Theorem. Multiply 1, ω, ω^2 by 1, then by ω and then by ω^2 and you will obtain three permutations whose first line will be 1, ω, ω^2

$$\therefore \text{ for } 1 \quad P_1=\begin{pmatrix}1 & \omega & \omega^2\\ 1 & \omega & \omega^2\end{pmatrix}=I$$

$$\text{for } \omega \quad P_2=\begin{pmatrix}1 & \omega & \omega^2\\ \omega & \omega^2 & \omega^3\end{pmatrix}=\begin{pmatrix}1 & \omega & \omega^2\\ \omega & \omega^2 & 1\end{pmatrix}$$

$$=(1 \quad \omega \quad \omega^2)$$

$$\text{for } \omega^2 \quad P_3=\begin{pmatrix}1 & \omega & \omega^2\\ \omega^2 & \omega^3 & \omega^4\end{pmatrix}=\begin{pmatrix}1 & \omega & \omega^2\\ \omega^2 & 1 & \omega\end{pmatrix}$$

$$=\begin{pmatrix}1 & \omega^2 & \omega\\ \omega^2 & \omega & 1\end{pmatrix}=(1 \quad \omega^2 \quad \omega)$$

It will be convenient to form a composition table of this group.

	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

The three permutations P_1, P_2, P_3 are obtained by

taking first row of composition table with each of the other three rows.

The permutation group $P=\{P_1, P_2, P_3\}$ and given group G are isomorphic by cayley's theorem.

2. *Find the regular permutation group isomorphic to the multiplicative group* $\{1, -1, i, -i\}$.

Let us form the composition table

.	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Each of the four lines denotes the first line multiplied by 1, -1, i and $-i$ respectively.

Hence by cayley's theorem the regular permutation group is of the four permutations which are obtained by taking first row with each of the four other rows.

$$\therefore \quad P_1=\begin{pmatrix} 1 & -1 & i & -i \\ 1 & -1 & i & -i \end{pmatrix}=I$$

$$P_2=\begin{pmatrix} 1 & -1 & i & -i \\ -1 & 1 & -i & i \end{pmatrix}=(1, -1)(i, -i)$$

$$P_3=\begin{pmatrix} 1 & -1 & i & -i \\ i & -i & -1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & i & -1 & -i \\ i & -1 & -i & 1 \end{pmatrix}$$

$$=(1 \quad i \quad -1 \quad -i)$$

$$P_4=\begin{pmatrix} 1 & -1 & i & -i \\ -i & i & 1 & -1 \end{pmatrix}=\begin{pmatrix} 1 & -i & -1 & i \\ -i & -1 & i & 1 \end{pmatrix}$$

$$=(1 \quad -i \quad -1 \quad i)$$

The permutation group $P=\{P_1, P_2, P_3, P_4\}$ and given group G are isomorphic to each other by Cayley's theorem.

3. *Find the regular permutation group isomorphic to the group* $G=\{a, b, c, d\}$ *with the composition table.*

∘	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Proceeding as in Ex. 2 the regular permutation group consists of the following four permutations P_1, P_2, P_3, P_4, which are obtained by taking the first line of composition table with each of the other four lines.

$$P_1=\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}=I$$

$$P_2=\begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}=(a\ b)\ (c\ d)$$

$$P_3=\begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}=\begin{pmatrix} a & c & b & d \\ c & a & d & b \end{pmatrix}=(a\ c)\ (b\ d)$$

$$P_4=\begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}=\begin{pmatrix} a & d & b & c \\ d & a & c & b \end{pmatrix}=(a\ d)\ (b\ c)$$

4. *Find the regular permutation group isomorphic to the group.*

$$G=[\{f_1, f_2, f_3, f_4\}, o]$$

where $f_1(z)=z$, $f_2(z)=-z$, $f_3(z)=1/z$, $f_4(z)=-1/z$.

The composition table has already been found on Page 29 It is same as of Ex. 3 if we replace a, b, c, d by $f_1, f_2, f_3,$

f_4 respectively. Hence the regular permutation group consists of the following four permutations.

$P_1=I$, $P_2=(f_1 f_2)\ (f_3 f_4)$, $P_3=(f_1 f_3)\ (f_2 f_4)$, and $P_4=(f_1 f_4)\ (f_2 f_3)$.

§ 19. Cyclic groups. **(Punjab 65)**

Def. *A group capable of being generated by a single element a is called a cyclic group and this single element is called its generator and the group is denoted as* $\{a\}$.

(Lucknow 66; Pb. 65; Bombay 70; Meerut 71; Marthwada 71; Kanpur 69)

Alternatively we can say that any element of a cyclic group can be expressed as a^n *or* na, n being any integer according as it is multiplicative group or additive group.

$\{a\}=\{\ldots -3a, -2a, -a, 0a=0=e, a, 2a. 3a \ldots\}$ for additive composition

or $\{a\}=\{\ldots a^{-3}\ a^{-2}, a^{-1}\ a^0=e, a^{-1}, a^{-2}, a^{-3}\ldots\}$ for multiplicative composition.

Theorem. 18. *To show that if a is a generator of a cyclic group then inverse of a is also its genera or.*

If a is a generator of the cyclic group then a^n is some integral power of a and it can be expressed as $(a^{-1})^{-n}$ showing that it is some integral power of a^{-1} and as such a^{-1} is also its generator.

Similarly for additive cyclic group generated by a any element na can be expressed as $-n\ (-a)$ *i.e.* it is some multiple of $-a$ and hence $-a$ is also a generator of the group.

Theorem. 19. *If the order of an element of a group G be n i e.* $a^n=e$ *then the set* $H=\{a, a^2, a^3, .., a^n=e\}$ *form a group w.r.t. the composition in G.*

Let $a^p, a^q \in H$ then $a^p.a^q=a^{p+q}=a^s \in H$

when $p+q=s \pmod n$ as $a^n=e$ given. Hence closure property.

Again $(a^p.a^q).a^r = a^{p+q}.a^r$

$= a^{(p+q)+r}$

$= a^{p+(q+r)} = a^p.a^{q+r} = a^p\ (a^q.a^r)$

Hence associative.

Also $(a^p)^{-1} = a^{-p} = a^{n-p}$ $\because$ $a^n = e$

Thus inverse exists and belongs to the set. Identity is given to be e. Hence the set H forms a group. Again as all the elements of H are generated from a therefore H is a cyclic group.

Exercise No. 7

1. *Prove that the group* $[\{1, -1, i, -i\}.]$ *is cyclic and find its generators.*

We observe that $(i)^1 = i$, $(i)^2 = -1$, $(i)^3 = -i$, $(i)^4 = 1$.

Thus all the elements can be expressed as integral powers of i and as such it is cyclic group whose generator is i.

Again $i^{-1} = -i$ *i.e.* inverse of i is $-i$

$\because$ $i\,(-i) = (-i)\ (i) = -i^2 = 1 =$ Identity,

Therefore $-i$ is also its generator by Th. 18 as can be verified

$(-i)^1 = -i$, $(-i)^2 = +1$, $(-i)^3 = i$, $(-i)^4 = 1$.

The above group consists of 4, 4th roots of unity.

Similarly we can show that the group $\{1, \omega, \omega^2\}$. consisting of three cube roots of unity is also cyclic whose generators are ω and ω^2. Also the multiplicative group consisting of n, nth roots of unity is also cyclic whose generators are $e^{(2\pi i)/n}$ and $e^{-(2\pi i)/n}$. **(Allahabad 70)**

2. *Prove that the additive group* $[\{0, 1, 2, 3, 4\}_{+5}]$ *is cyclic and find its generators.*

Clearly 1 is a generator of this group as each element is a multiple of 1.

Again $1 +_{+5} 4 = 4 +_{+5} 1 = 5 =_{+5} 0$ identity

Therefore 4 is inverse of 1 and as such it is also its generator by Th. 18. as can be verified below

$$0.4=0,\ 1.4=4,\ 2.4=\underset{+5}{8}=3,\ 3.4=\underset{+5}{12}=2,\ 4.4=\underset{+5}{16}=1$$

Thus all the elements are multiples of 4 under the given composition.

It may also be verified that 2 and its inverse 3 are also its generators.

We can similarly prove that the group

$G=\{(0, 1, 2, 3, m-1)\}_{,+m}$ is *a* cyclic group whose generator is 1 and the other generator is $m-1$.

3. *Prove that the multiplicative group*

$$[\{1, 2, 3, 4\}_{\times 5}] \textit{ is cyclic}$$

and find its generators.

$$2^0=1,\ 2^1=2,\ 2^2=4,\ 2^3=\underset{\times 5}{8}=3.$$

Thus all the elements are integral powers of 2 and hence 2 is its generator.

Also $2\times 3=3\times 2=\underset{\times 5}{6}=1=$identity.

$\therefore$ 3 is the inverse of 2 and as such 3 is also its generator by Th. 18 as shown below

$$3^0=1,\ 3^1=3,\ 3^2=\underset{\times 5}{9}=4,\ 3^3=\underset{\times 5}{27}=2 \text{ etc.}$$

4. *Prove that every isomorphic image of a cyclic group is again cyclic.* **(Punjab 65, 70)**

Let G be a cyclic group generated by a so that a^n be its element. G' is its isomorphic image under an isomorphism f.

$$a^n \in G \text{ and } f(a^n) \in G'$$

$f(a^n)=f(a\cdot a.a.....n \text{ factors})$

$=[f(a).f(a).f(a)\ldots\ldots n \text{ factors}]$ by def. of f

$=[f(a)]^n$.

Hence every element $f(a^n) \in G'$ can be expressed as an integral power of its element $f(a)$ which therefore is a generator of G' Hence G' is cyclic.

5. *If G be the group $\{0, 1, 2, 3, 4\}$ under addition modulo 5 and G' the cyclic group of order 5 $\{a, a^2, a^3, a^4, a^5 = e\}$ then prove that the mapping $f: G \to G' : f(m) = a^m$, $m \in G$ is an isomorphism of G onto G'.*

The mapping f is clearly one-one-onto. For isomorphism we have only to prove that f preserves the group compositions.

$$3 +_{+5} 4 = 7 = 1 \cdot 5 + 2,\ 2 + 4 = 6 = 1 \cdot 5 + 1$$

In general if $m, n \in G$ then $m + n = 5p + r$

where $0 \leqslant r < 5$

Hence $m +_{+5} n = r \quad \therefore\ f(m +_{+5} n) = f(r)$ ...(1)

Again $f(m)\, f(n) = a^m . a^n = a^{m+n} = a^{5p+r} = (a^5)^p . a^r = a^r$

$\because \quad a^5 = e$

or $f(m)\, f(n) = f(r)$ ...(2)

Hence from 1 and 2 we get

$$f(m+n) = f(m)\, f(n)$$

Hence f preserves group compositions which therefore is an isomorphism.

Certain Theorems on cyclic groups

Theorem. 20. Every cyclic group is abelian.

Let G be a cyclic group being generated by a and let x and y be its two elements then

$$x = a^r,\ y = a^s$$

$$xy = a^r\, a^s = a^{r+s} = a^{s+r}\, a^s\, a^r = yx$$

Hence $xy = yx \quad \forall\ x, y \in G \quad \therefore \quad G$ is abelian.

Theorm 21. *If the generator of a cyclic group G is of infinite order (or zero oder), then G has exactly two generators and is isomorphic to the additive group of integers.*

(B. H. U. 69; Punjab 65, 67)

Since the order of the generator a is zero, then no two powers of a shall be same because if possible let $a^r = a^s$ where $r > s$.

$$\therefore \quad a^r . a^{-s} = a^s . a^{-s} = a^0 = e.$$

or
$$a^{r-s} = e.$$

But this is not possible as the order of a is zero and as such r must be s which is a contradiction

$$\therefore \quad a^r \neq a^s$$

Hence the cyclic group G contains infinite number of terms.

$$\therefore \quad G = \{\ldots a^{-r} . a^{-2}, a^{-1}, a^0, a, a^2 \ldots a^r \ldots\}$$

If a^r is an element of group G then $a^r = (a^{-1})^{-r}$. Thus a^{-1} is also a generator of G and as shown above no two powers of of a shall be same, Therefore a and a^{-1} are two distinct generators. In order to show that it has exactly two generators we have to show that it cannot have any other generator except a and a^{-1}. For if possible let us suppose that a^m $(m \neq 1, -1)$ is a generator of G, then there must exist an integer k such that $(a^m)^k = a$. *i.e.* $a^{mk} = a$. But since $m \neq 1, -1$ therefore $mk \neq 1$ and hence $a^{mk} = a \Rightarrow$ that two distinct $(mk \neq 1)$ powers of a are equal which is a contradiction as we have proved that no two powers of a shall be same. Hence a^m $(m \neq 1, -1)$ cannot be a generator of G. Hence G has exactly two generators which are a and a^{-1}.

Let I be the additive group of integers

$$I = \{\ldots -r, \ldots -2, -1, 0, 1, 2 \ldots\ldots r \ldots\ldots\}$$

We have to show that $G \cong I$ and for this we have to show

the existence of one-one mapping f of G onto I which preserves the group compositions.

Let us define $f : G \to I : f(a^r) = r, r \in I$.

The mapping f is clearly one-one because

$$f(a^r) = f(a^s) \Rightarrow r = s$$

and it is also onto,

Now $f(a^r . a^s) = f(a^{r+s}) = r + s = f(a^r) + f(a^s)$.

i.e., the mapping preserves the group compositions.

Hence $G \cong I$.

Theorem 12. *If a generator a of a cyclic group G is of order $n > 0$, then G has exactly n distinct elements. Also prove that G is isomorphic to the additive group of residue classes modulo n.* **(Meerut 71; Poona 70; Punjab 65, 67, 70)**

I Part. Since n is the order of generator a then $a^n = e$ where n is the least +ive integer satisfying the above relation.

Now we shall show that the group G consists of exactly n elements namely $a, a^2, a^3, \ldots, a^n = e$. ...(1)

Let s be any integer greater than n and G contains the element a^s.

Then by division algorithm $s = nq + r$ where $0 \leqslant r < n$.

$\therefore \quad a^s = a^{nq+r} = a^{nq} . a^r = (a^n)^q \, a^r = a^r \quad \because \quad a^n = e$

but r is less than n and a^r is contained in (1) and hence the set shall not contain more than n elements.

Now we shall establish that it contains exactly n etements by showing that no two elements of (1) are same for if possible let

$$a^r = a^q \text{ where } 0 < r < q < n.$$

$\therefore \quad a^r . a^{-r} = a^q . a^{-r} \Rightarrow a^0 = a^{q-r}$,

or $a^{q-r} = e$ where $q - r$ is +ive integer less than n.

But this is not possible because n is the order of a and as such there can not be any other integer $q - r$ less than n

such that $a^{q-r}=e$. Hence $a^{q-r} \neq e$ and consequently $a^r \neq a^q$ showing thereby that all the elements listed in (*I*) are distinct. Hence the group G consists of exactly n elements.

II. Part. $\therefore$ $G=[a, a^2, a^3, \ldots\ldots, a^n=e]$.

$G'=[\{1\}, \{2\}, \ldots\ldots, \{n\}=\{0\}]$

addition of residue classes mod. n.

Let us define a mapping $f: G \to G'$ such that $f(a^r)=\{r\}$

The mapping is clearly one-one onto

$$f(a^r . a^s)=f(a^{r+s})=\{r+s\}=\{r\}+\{s\}$$

by the definition of sum of residue classes

$$=f(a^r)+f(a^s).$$

Therefore the mapping f preserves the group compositions.

Theorem 23. *A cyclic group G with a generator of finite order n, $n > 0$ has exactly n elements and is isomorphic to the multiplicative group of n, nth roots of unity.*

As in last theorem 22 we shall establish that the set G consists of exactly n elements

$G=\{a, a^2, a^3, \ldots, a^n=e\}$

As shown in **Ex. 19 P. 24** the n, nth roots of unity form a group

$$G'=\left\{e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots \quad e^{\frac{2r\pi i}{n}} \ldots\ldots e^{\frac{2n\pi i}{n}}=1\right\}$$

Let us define $f: G \to G'$, $f(a^r)=e^{\frac{2r\pi i}{n}}$

The mapping is one-one as $f(a^r)=f(a^s) \Rightarrow$

$$e^{\frac{2r\pi i}{n}}=e^{\frac{2s\pi i}{n}}$$

$$\Rightarrow r=s \Rightarrow a^r=a^s.$$

Also it is clearly onto.

Now $f(a^r . a^s)=f(a^{r+s})=e^{\frac{2\pi i (r+s)}{n}}$

$$e^{\frac{2\pi ri}{n}} . e^{\frac{2\pi si}{n}} = f(a^r) . f(a^s).$$

Hence the mapping f preserves the group compositions.

$$\therefore \qquad G \cong G'.$$

Theorem 24. *If a cyclic group is generated by an element a of order n then a^m is a generator iff $(m, n)=1$ i.e. g. c. d. of m and n is 1* **(Gorakhpur 70; Bombay 70)**

$$o(a)=n \Rightarrow a^n=e \qquad \ldots(1)$$

g. c. d. of $m, n=1 \Rightarrow \exists$ two integers p and q such that

$$pm+qn=1 \qquad \ldots(2)$$

Let H be the set which is generated by a^m then as any element of H is $(a^m)^k=a^{mk}$ which belongs to G the cyclic group generated by a.

$$\therefore \qquad H \subseteq G \qquad \ldots(3)$$

Again $a^{pm+qn}=a$ by (2)

$\therefore \quad a^{pm} . a^{qn}=a \Rightarrow (a^m)^p . e^q=a$ by (1) $\therefore \quad (a^m)^p=a$

Above shows $a \in G$ is expressible as integral power of a^m and as such it belongs to H

$$\therefore \qquad G \subseteq H \qquad \ldots(4)$$

Hence from (3) and (4) we get $G=H$

Conversely : Given a^m is a generator of G, to prove that g. c. d. of m, n is 1.

Let g. c d. of m, n be d, therefore d divides both m and n i.e. m/d and n/d are +ive integers.

Now $(a^m)^{n/d}=(a^n)^{m/d}=(e)^{m/d}=e$

$$\therefore \qquad o(a^m)=\frac{n}{d} < n.$$

and hence a^m cannot be a generator of G, which contradicts that a^m is a generator of onder n.

Hence $d=1$

Therem 25. *Any two cyclic groups of the same order are isomorphic.*

Let G_1 and G_2 be two cyclic groups of the same finite order say n so that both of them have exactly n elements. In other words the order of generator in each is n. Hence by theorem 22 P. 125. each of them is isomorphic to the additive group G_3 of residue classes modulo m

$\therefore \quad G_1 \cong G_3 , \quad G_2 \cong G_3 \Rightarrow G_3 \cong G_2$ (symmetric).

Both the above imply that $G_1 \cong G_2$ (Transitive) as we know that the relation of isomorphism is an equivelence relation *i e.* reflexive, symmetric and transitive

Again if order of G_1 and G_2 be infinite then order of generator of each is i finite and by 21 P. 124 each is isomorphic to additive group G_3 of integers

$\therefore \quad G_1 \cong G_3, G_2 \cong G_3 \Rightarrow G_3 \cong G_2$ (symmetric)

Both the above imply that $G_1 \cong G_2$ (Transitive) as above

---

List of Imortant Questions and Articles.

§ 3 P. 6, **Exercise 1 P. 8 Q** [1, 8, 9, 11, 12, 13. 15 (a), 16, 19, 21, 22]. Th. I P. 35, **Th.** 2 P. 38, **Th.** 3 P. 43, Th. 5 P. 44.

§ 6 P. (45–50) all properties. **Th.** 6 **P.** 51, **Th.** 4 **P.** 57, Th. 7 P. 67, § 10 P. 70, Th. 8 P. 71, Ex 2 P. 74, Ex 3 P. 75 § 12 P. 79, Th. 10, 11, 12, 13 P. (81–84), **Ex 4 P. (84–91)** Q [1, 3, 4, 9, 11, 12] § 14 P. 91, § 16 P. 94. **Ex 5 P. (95–108)** Q [4, 6, 7, 10, 14, 15.] § 16, P, 108 Th. 15 P. 110 Th. 17 P. 114, **Exercise 6 P. (117–119)** Q. [?, 4], § 19 P. 120

Exercise 7 P. **121–124.** Q [1, 4] Th. 21 P. 124 Th. 22 P. 125 Th. 24 P. 127,

CHAPTER II
SUB GROUPS

§ 1. Sub groups :

Let H be a non empty sub set of a group G in which the group composition is denoted multiplicatively Again let a and b be any two elements of H which are also the elements of G. Since G is a group ab must belong to G but it is not necessary that ab may belong to H also, when a and $b \in H$.

Stable. In case when $a, b \in H \Rightarrow ab \in H$ then we say that H is stable for the composition in G *i.e* , the composition in G has induced the composition in H, *i.e.*, H and G have the same binary composition.

Sub group. *A non empty sub set H of a group G is said to be a sub group of G if*

(*1*) *H is stable in G i e , composition in G induces composition in H i e , $ab \in H \ \forall \ a, b \in H$.*

(*2*) *H satisfies all the postulates of a group for the induced composition.*

(Lucknow 67; 68, 69; Meerut 69)

Proper and improper sub groups :

Every group G has two trivial sub groups *i.e.*, G itself and the identity group consisting of single element e and these two are called improper sub groups and the rest all are called proper sub groups.

Complex. Any non empty sub set H of a group G whether it is a sub group or not is called a complex. Thus every sub group H of G is a complex but every complex is not a sub group.

Examples of sub groups :

1. G=[All vectors in three dimensions +]
   H=[All plane vactors +]
2. G=[All integers +]
   H=[Even integers +]
3. G=(non zero real numbers ×)
   H=(+ive rational numbers ×)
4. G=($2n$, $2n$th roots of unity ×)
   H=(n, nth roots of unity ×)
5. G=(All real numbers, +)
   H=(All +ive real numbers ×) **Gujrat 70**

Not sub group.

Here in Ex. 5 H is though a sub-set of G and is a group of its own, but it is not a sub group because the composition in G and H are different.

§ 2 The identity, inverse and order of an element of a sub group H.

(*a*) *The identity of a sub group H of G is the same as that of G.*

(*b*) *The inverse of any element of H is the same as the inverse of that element regarded as an element of group G.*

(*c*) *The order of any element of H is the same as the order of that element regared as an element of group G.*

(a) Let $a \in H$ and e' be the identity of H.
Then $a\,e' \in H$ by def. of H.
Also $a\,e'=a$ ...(1)
Again $a \in H \Rightarrow a \in G$ and if e be the identity of G.
Then $a\,e=a$ .. (2)
Hence from (1) and (2) we get

$a\,e' = a\,e \Rightarrow e' = e$ by L. can. Law.

(b) Let e be the identity of both G and H by (*a*)

$a \in H \Rightarrow a \in G$ and suppose b is the inverse of a in H and c is the inverse of a in G then by def.

$a\,b = e$ and $a\,c = e \Rightarrow a\,b = ac \Rightarrow b = c$ by L. C. Law.

(c) Since the identities of both H and G are same, we can easily establish that the order of element $a \in H$ is the same as the order of a regarded as a member of G.

§ 3. Criteria for a sub group

Theorem 1. *A non empty sub-set H of a group G is a sub group of G if and only if*

(*i*) $a \in H, b \in H \Rightarrow a\,b \in H$

(*ii*) $a \in H \Rightarrow a^{-1} \in H$ *where* a^{-1} *is the inverse of* a *in* G. **(Lucknow 68, 70; Allahabad 66, 69)**

The conditions are necessary. H is a sub group and hence it must be closed with respect to the composition in G.

$\therefore\ a \in H,\ b \in H \Rightarrow a\,b \in H$

which proves condition (i)

Let $a \in H$ then its inverse a^{-1} is the same as the inverse of a regarded as an element of G. Since H is a sub group therefore inverse of $a \in H$ *i.e.* a^{-1} must also belong to H.

The conditions are sufficient Given the conditions (i) and (ii) hold, to prove that H is a sub group of group G.

Closure property.

By (i) $a \in H, b \in H \Rightarrow a\,b \in H$. Hence H is closed with respect to multliplication composition.

Associative.

Again H being a sub set of G in which the composition

is associative and hence it follows that the induced composition in H isalso associative.

Identity. We know that identity of the sub group H is the same as the identity of G. The only thing we have to see that the identity belongs to H.

By (ii) $a \in H \Rightarrow a^{-1} \in H$.

By (i) $a \in H,\ a^{-1} \in H \Rightarrow a\,a^{-1} \in H \Rightarrow e \in H$.

Inverse. By (ii) $a \in H \Rightarrow a^{-1} \in H$. Hence each element of H has an inverse which is in H.

Thus all the postulates of a group are satisfied and hence H is a sub group.

Theorem 2. *The necessary and sufficient condition that a non empty sub set H of a group G be a sub group is*

$$a \in H, b \in H \Rightarrow ab^{-1}\ H$$

(Delhi Hons. 70; Aligurh 65; Allahabad 65; Punjab 70; Meerut 71; Utkal 69; Marthwada 70)

The condition is necessary.

i.e., H is a sub group, *i.e.* it satisfies the postulates of a group and $a,\ b \in H$ and we will show that $ab^{-1} \in H$,

Since $b \in H \ \therefore\ b^{-1} \in H \ \because\ H$ is a group by itself, therefore inverse of every element exists and belongs to H.

Now $a \in H$ and $b^{-1} \in H \Rightarrow ab^{-1} \in H$ by closure property in H which is a group.

The condition is sufficient.

Here we are given

$$a \in H, b \in H \Rightarrow ab^{-1} \in H.$$

we have to show that H is a sub group, *i.e.* it satisfies all the postulates of a group for the induced composition, *i.e.* closure, associative, identity and inverse.

$$a \in H, b \in H \Rightarrow ab^{-1} \in H \text{ (given).} \qquad \ldots(1)$$

Choosing $b=a$, $a \in H, a \in H \Rightarrow aa^{-1} \in H \Rightarrow e \in H$, where e is the identity of G. Hence identity exists.

Again $e \in H$ and $a \in H \ \therefore \ ea^{-1}=a^{-1} \in H$ by (1).

Hence the inverse of every element exists and belongs to H.

Again $b \in H$ and $b^{-1} \in H$ as shown above.

Also $a \in H$ and $b^{-1} \in H$, $\therefore$ $a\,(b^{-1})^{-1} \in H$ by (1) or $ab \in H$, *i.e.* closure property.

This establishes that H is stable for the composltion in G, *i.e.* H and G have the same composition. Since composition in G is assosiative, G being a group therefore composition in H is also associative. Thus all the group postulates are satisfied and hence H is a sub group.

Note. **In multiplicative notation** the condition for a sub group has been proved to

$$a \in H, b \in H \Rightarrow ab^{-1} \in H.$$

In **additive notation** we shall express it as

$a \in H, b \in H \Rightarrow a-b \in H$,

as $-b$ is the inverse of b in additive notation.

Ex. 1 *Let G be the additive group of integers, then prove that the set of all multiples of integers by a fixed integer m is a sub group of G.*

$G=\{\ldots,-3, -2, -1, 0, 1, 2, 3,\ldots\ldots\}+$.

$H=\{\ldots-3m, -2m, -m, 0, m, 2m, 3m, \ldots\ldots\}+$.

Let $A=rm$, $B=sm$ be any two elements of H where r and s are integers. Also $B^{-1}=-B=-sm$ as G is additive group.

$AB^{-1}=A-B=rm-sm=(r-s)\,m=p\,m$ where p is an integer. Hence by Theorem 2 P. 132 H is a sub group.

Ex. 2. *Let a be an element of a group G. The set* $H=\{a^n : n \in I\}$ *of all integral powers of a is a sub group of G.*

$H=\{..., a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, ...\}$

Let $A=a^r, B=a^s$ be any two elements of H. Where r and s are integers.

Also $B^{-1}=(a^s)^{-1}=a^{-s}$

$\therefore$ $AB^{-1}=a^r a^{-s}=a^{r-s}=a^p$ when p is some integer and as such belongs to H. Thus $A \in H, B \in H \Rightarrow AB^{-1} \in H$ and hence H is a sub group by **Th 2 P. 132.**

Theorem 3. For finite groups.

The necessary and sufficient condition for a non empty sub set H of a **finite group G** *to be a sub group is*

$$a \in H, b \in H \Rightarrow ab \in H$$

i.e. closure property is satisfied.

(Lucknow 67; B. H. U 70; Meerut M. Sc. 68; B. Sc. 69)

The condition is necessary.

Given that H is a sub group to show that

$$a \in H, b \in H \Rightarrow ab \in H.$$

Since H is a sub group, it is stable

i.e., $$a \in H, b \in H \Rightarrow ab \in H.$$

The condition is sufficient.

Given that $a \in H, b \in H \Rightarrow ab \in H$, to prove that H is a sub group. *i.e.* it satisfies the postulates of a group.

Let $a \in H$, then $a \in G$ also which is finite and hence its order must be finite, say it is n, so that $a^n=e$, where n is the smallest +ive integer satisfying the above relation.

Now $a \in H, b \in H \Rightarrow ab \in H$ given.

Choosing $b=a$, $\therefore$ $a \in H, a \in H \Rightarrow a^2 \in H$.

$$a \in H, a^2 \in H \Rightarrow a.a^2=a^3 \in H.$$

Continuing like this we can say that

$$a^n \in H, \textit{ i.e. } e \in H.$$

Identity exists and belongs to H.

Again as shown above.

$$a^{n-1} \in H \Rightarrow a^n.a^{-1} \in H$$

or $$ea^{-1} \in H \Rightarrow a^{-1} \in H.$$

Thus inverse of an element $a \in H$ exists and belongs to H.

Therefore the sub set H satisfies the closure property as given, possesses identity and inverse also exists for every element belonging to H. The associative property is implied as the composition in G being associative and H has the same composition as of G.

Hence H is a sub group.

Note. The above theorem holds only for finite groups and not for infinite groups.

Ex 1. $G=[\textit{All integers} \quad +]$

$H=[\textit{All +ive integers} \ +]$

Clearly H is a sub set of G and also the closure property is satisfied *i.e.* sum of two +ive integers is again a +ive integer but still it is not a sub group as the inverse of +ive integers will not exist for additive composition in H and also the identity element $0 \notin H$.

Ex. 2. $G=\{..., 2^{-3}, 2^{-2}, 2^{-1}, 1, 2, 2^2, 2^3 .. \times\}$, *G is a multiplicative group.*

$H=\{1, 2, 2^2, 2^3, ...\}$ is a sub set of G in which closure property is satisfied but still H is not a sub group as the inverse of elements of H does not belong to the set H

i.e. $(2^2)^{-1}=2^{-2} \notin H$.

Exercise 1

Ex. 1. *The set of* $\frac{1}{2}.n\,!$ *even permutations on n symbols is a sub group of the symmetric group* S_n *on n symbols as we know that the product of two even permutations is again an even permutation thus the closure property is satisfied.* (*Th, 3*). *This sub group is called the* **alternating group** A_n *on n symbols and it is of order* $\frac{1}{2}.\,n\,!$. **(Raj. M Sc. 66)**

Ex 2. *Show that in a group G all those elements x which commute with every element of G form a sub group of G called the* **centre** *of G i.e.*

$$X=\{x : x \in G \text{ and } xa=ax \ \forall\ a \in G\}.$$

Criteria for a sub group H is

$$a \in H, b \in H \Rightarrow ab^{-1} \in H. \qquad \textbf{(Th. 2 P, 132)}$$

X is a sub set of G and let $x_1, x_2 \in X$ and any arbitrary $a \in G$ then $ax_1=x_1a$, $ax_2=x_2a$ given. In order to prove that X is a sub group of which two elements are chosen to be x_1, x_2 we shall establish that $x_1x_2^{-1} \in X$ and hence it will be sub group.

We are given that $x_2a=ax_2 \quad \forall\ a \in G$

$$\Rightarrow x_2^{-1}\,(x_2a)\,x_2^{-1}=x_2^{-1}\,(ax_2)\,x_2^{-1}$$
$$\Rightarrow (x_2^{-1}x_2)(ax_2^{-1})=(x_2^{-1}a)\,(x_2x_2^{-1})$$
$$\Rightarrow e\,(ax_2^{-1})=(x_2^{-1}a)\,e \Rightarrow ax_2^{-1}=x_2^{-1}a. \qquad \ldots(1)$$

i.e. x_2^{-1} also commutes with $a \ \forall\ a \in G$ and hence $x_2^{-1} \in X$.

Now $(x_1\,x_2^{-1})\,a=x_1\,(x_2^{-1}\,a)=x_1\,(a\,x_2^{-1})$ by 1

$$=(x_1\,a)\,x_2^{-1}=(a\,x_1)\,x_2^{-1}$$

$$\because \quad x_1\,a=a\,x_1$$

$$=a\,(x_1\,x_2^{-1}).$$

Thus $(x_1\,x_2^{-1})\,a=a\,(x_1\,x_2^{-1})$.

Above shows that $x_1 x_2^{-1}$ also commutes with $a \forall a \in G$ and as such it belongs to X.

Thus $x_1, x_2 \in X \Rightarrow x_1 x_2^{-1} \in X$ and hence X is a sub group.

Ex. 3. *Let $N(a)$ be the set of all those elements x of a group G which commute with a fixed element 'a' of G then $N(a)$ is a sub group of G i.e. $N(a)=\{x : x \in G \text{ and } ax=xa\}$.*

(Delhi 70; Punjab 70; Lucknow 69)

Clearly $N(a)$ is non empty as $e \in G$ and $e\,a=a=ae=a$

i.e. $e \in N(a)$.

Let $x_1, x_2 \in N(a)$ so that

$$a\,x_1=x_1\,a \text{ and } a\,x_2=x_2\,a \qquad \ldots(1)$$

Now $x_2\,a=a\,x_2 \Rightarrow x_2^{-1}(x_2\,a)\,x_2^{-1}=x_2^{-1}(a\,x_2)\,x_2^{-1}$

$$\Rightarrow (x_2^{-1}\,x_2)\,a\,x_2^{-1}=(x_2^{-1}\,a)\,(x_2\,x_2^{-1})$$

$$\Rightarrow a\,x_2^{-1}=x_2^{-1}\,a. \qquad \ldots(2)$$

Above implies that x_2^{-1} also commute with $a \in G$ and as such x_2^{-1} also belongs to $N(a)$.

Now $(x_1 x_2^{-1})\,a=x_1(x_2^{-1}\,a)=x_1(a\,x_2^{-1})$ by (2)

$$=(x_1\,a)\,x_2^{-1}=(a\,x_1)\,(x_2^{-1})$$

$\because\ a\,x_1=x_1\,a$ by (1).

$\therefore \quad (x_1 x_2^{-1})\,a=a\,(x_1 x_2^{-1})$.

Hence $x_1 x_2^{-1}$ also commutes with a and as such it belongs to $N(a)$.

Thus $x_1, x_2 \in N(a) \Rightarrow x_1 x_2^{-1} \in N(a)$

which therefore is a sub group.

Ex. 4. *Prove that those elements of a group G which commute with the square of a given element a of G form a sub group H of G and those which commute with a itself form a sub group of H.*

$H=\{x : x \in G \text{ and } a^2x=xa^2\}$.

In order to show H is a sub group of G we have to proceed exactly as in Ex. 2 and 3.

Let $N=\{x : x \in G \text{ and } a\,x=x\,a\}$.

Note. In Ex. 3 we had proved the above set to be a sub group of G but here we have to prove it to be a sub group of H

Method. We shall show that N is non empty. N is a sub set of H and lastly if $x_1, x_2 \in N$ then $x_1\,x_2^{-1}$ also belongs to N.

Since $ae=e\,a=a$.

$\therefore$ $e \in N$ and as such it is non empty.

Now let $x \in N \Rightarrow x\,a=a\,x$

$\Rightarrow (x\,a)\,a=(a\,x)\,a \Rightarrow x\,a^2=a\,(x\,a)$

$\Rightarrow (x\,a^2)=a\,(a\,x) \Rightarrow x\,a^2=a^2\,x$.

i.e. x commutes with a^2 and hence $x \in H$.

$\therefore$ $x \in N \Rightarrow x \in H$ $\therefore$ $N \subseteq H$.

Hence N is a non empty sub set of H.

Now we should as in Ex. 3 prove that when $x_1, x_2 \in N$ $x_1\,x_2^{-1}$ also belongs to N which therefore is a sub group of H.

Ex. 5. *Let H be a sub group of G and*

$$T=\{x : x \in G \text{ and } xH=Hx\}.$$

Prove that T is a sub group of G.

It is exactly as Ex. 3.

Let $x_1, x_2 \in T$. then $x_1\,H=H\,x_1$, $x_2\,H=H\,x_2$. ...(1)

Now $x_2\,H=H\,x_2 \Rightarrow x_2^{-1}\,(x_2\,H)\,x_2^{-1}=x_2^{-1}\,(H\,x_2)\,x_2^{-1}$

$\Rightarrow (x_2^{-1}\,x_2)\,(H\,x_2^{-1})=(x_2^{-1}\,H)\,(x_2\,x_2^{-1})$

$\Rightarrow H\,x_2^{-1}=x_2^{-1}\,H$. ...(2)

Above relation implies $x_2^{-1} \in T$.

Now $(x_1 x_2^{-1}) H = x_1 (x_2^{-1} H) = x_1 (H x_2^{-1})$ by (2)
$= (x_1 H) x_2^{-1} = (H x_1) x_2^{-1}$ by (1)
$= H (x_1 x_2^{-1})$.

Above relation implies $(x_1 x_2^{-1}) H = H (x_1 x_2^{-1})$.

$\therefore$ $x_1 x_2^{-1}$ also belongs to T when $x_1, x_2 \in T$ and hence T is a sub group.

Another form.

$$T = \{x : x \in G \text{ and } x H = H x\}$$
$$= \{x : x \in G \text{ and } x^{-1} x H = x^{-1} H x\}$$
$$= \{x : x \in G \text{ and } x^{-1} H x = H\}.$$

Ex. 6. *Let H be a sub group of a group G and let for $x \in G$, $x H x^{-1} = \{x h x^{-1} : h \in H\}$. Prove that $x H x^{-1}$ is a sub group of G.*

Let a and $b \in x H x^{-1}$.

$\therefore$ $a = x h_1 x^{-1}$, $b = x h_2 x^{-1}$ where $h_1, h_2 \in H$
and since h is a sub group $\therefore$ $h_1 h_2^{-1} \in H$. ...(1)

Now in order to show that $x H x^{-1}$ is a sub group we shall show that $a b^{-1} \in x H x^{-1}$ when $a, b \in x H x^{-1}$.

$$a b^{-1} = (x h_1 x^{-1}) (x h_2 x^{-1})^{-1}$$
$$= (x h_1 x^{-1}) (x^{-1})^{-1} (h_2)^{-1} (x)^{-1}$$
$$= (x h_1 x^{-1})(x h_2^{-1} x^{-1})$$
$$= x h_1 (x^{-1} x) h_2^{-1} x^{-1} = x h_1 e h_2^{-1} x^{-1}$$
$$= x (h_1 h_2^{-1}) x^{-1} = x h x^{-1}$$
where $h = h_1 h_2^{-1} \in H$.

But $x h x^{-1} \in x H x^{-1}$.
Hence $a b^{-1} \in x H x^{-1}$

which therefore is a sub group.

Ex. 7. *Let G be the set of all ordered pairs (a, b) of real numbers for which $a \neq 0$. Let a binary composition o be defined in G*

$$(a, b) \, o \, (c, d) = (ac, \; bc + d)$$

Show that (G, o) *is a non-commutative group.*

Prove further that the sub set H *of all those elements of* G *which are of the form* $(1, b)$ *form a sub group of* G.

(Raj. M.Sc. 69)

We have proved the first part in Ex. 17. P. 22 and where we have shown that $(a, \; b)^{-1} = \left(\frac{1}{a} \; , \; \frac{-b}{a} \right)$ ...(1)

Let $x, y \in H \quad \therefore \quad x = (1, a), y = (1, b)$

$$\therefore \quad xy^{-1} = (1, a) \, o \, (1, \; b)^{-1} = (1, a) \, o \left(1, \frac{-b}{1} \right) \text{ by I}$$

$$= (1, a - b) \text{ by definition of } o$$

$$\in H$$

Hence by theorem 2 P. 132. H is a sub group.

§ 4. Intersection of two sub groups.

Theorem 4. *The intersection of any two sub groups of a group* G *is again a sub group of* G. **(Meerut B.Sc. 70)**

Let H_1 and H_2 be any two sub groups and $H_1 \cap H_2$ be their intersection. In order to prove that $H_1 \cap H_2$ is a sub group we shall use Theorem 2 P. 132

i.e., $a, b \in H_1 \cap H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

$a \in H_1 \cap H_2 \Rightarrow a \in H_1, a \in H_2$

$b \in H_1 \cap H_2 \Rightarrow b \in H_1, b \in H_2$

$a \in H_1, b \in H_1 \Rightarrow ab^{-1} \in H_1 \quad \because H_1$ is a sub group

$a \in H_2, b \in H_2 \Rightarrow ab^{-1} \in H_2 \quad \because H_2$ is a sub group

$\therefore \quad ab^{-1} \in H_1, ab^{-1} \in H_2 \Rightarrow ab^{-1} \in H_1 \cap H_2$.

Hence $H_1 \cap H_2$ is a sub group.

Note. $H_1 \cap H_2$ is the largest sub group contained in H_1 as well as in H_2.

Also the intersection of sub groups can never be null as

there is at least one element *i.e.* identity element which is common to both the sub groups.

Generalisation of the theorem on intersection of two sub groups.

The intersection of any family of sub groups of a group G is again a sub group.

(Luck. 66, 69; Meerut 70; Raj. M.Sc. 66)

Let $A=\{H_1, H_2, H_3, \ldots \ldots\}$

where each H_i is a sub group of G.

Again let $H^*=\cap \{H_i : H_i \in A$ *i.e.* H_i is a sub group$\}$.

We have to show that H^* is a sub group for which we shall use the criteria of theorem 2 P. 132

i.e. $\quad a \in H, b \in H \Rightarrow ab^{-1} \in H.$

Let $a, b \in H^*$ then by definition of intersection

$$a \in H_i, b \in H_i \; \forall \; H_i \in A.$$

But each H_i is a sub group.

$\therefore \quad a \in H_i, b \in H_i \Rightarrow ab^{-1} \in H_i \; \forall \; H_i \in A.$

Hence $ab^{-1} \in H^*$.

Thus $a \in H^*, b \in H^* \Rightarrow ab^{-1} \in H^*$.

Hence H^* is a sub group.

§ 5. The union of sub groups.

The union $H_1 \cup H_2$ of two sub groups is generally not a sub group.

For example : $G=(\ldots -3, -2, -1, 0, 1, 2, 3 \ldots\ldots)+$

$H_1=(\ldots -4, -2, 0, 2, 4, \ldots)+$

$H_2=(\ldots -6, -3, 0, 3, 6 \ldots\ldots)+$

$\therefore \quad H_1 \cup H_2=(\ldots -6, -4, -3, -2, 0, 2, 3, 4, 6 \ldots)$

But $H_1 \cup H_2$ is not a sub group as it is not a group for induced composition

as $\quad 3, 4 \in H_1 \cup H_2$ but $3+4=7 \neq H_1 \cup H_2$

i.e., Closure property is not satisfied.

Theorem 5. *The union of two sub groups is a sub group if and only if one is contained in the other.*

Given. H_1, H_2 are any two sub groups such that

$$H_1 \subseteq H_2.$$

To prove. $H_1 \cup H_2$ is a sub group.

Clearly $H_1 \cup H_2 = H_2$ as $H_1 \subseteq H_2$.

Since H_2 is a sub group therefore $H_1 \cup H_2$ is also a sub group.

Converse. Given $H_1 \cup H_2$ is a sub group.

To prove that either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

Let us suppose that neither $H_1 \subseteq H_2$ nor $H_2 \subseteq H_1$.

Since $H_1 \not\subseteq H_2 \Rightarrow \exists\, a \in H_1$ but $a \notin H_2$. ...(1)

Similarly $H_2 \not\subseteq H_1 \Rightarrow \exists\, b \in H_2$ but $b \notin H_1$. .. (2)

Therefore from (1) and (2) we get

$$a \in H_1 \cup H_2,\ b \in H_1 \cup H_2.$$

But $H_1 \cup H_2$ is a sub group and hence

$$a\,b \in H_1 \cup H_2. \qquad \text{Th. 3 P. 134}$$

From above it follows that $a\,b \in H_1$ or $ab \in H_2$.

Let $ab \in H_1$ then $a^{-1}\,ab \in H_1 \Rightarrow b \in H_1$ which contradicts (2).

Hence either $H_1 \subseteq H_2$ or $H_2 \subseteq H_1$.

[When $a \in H_1$ then $a^{-1} \in H_1$ and hence $a^{-1}\ (ab) \in H_1$ as H_1 is a sub group].

§ 6. Algebra of Complexes of a group.

(a) Multiplication of two complexes H_1 and H_2 (not sub groups) of a group G.

$H_1\,H_2 = \{h_1\,h_2 : h_1 \in H_1 \text{ and } h_2 \in H_2\}$

Since $h_1 \in H_1$ and H_1 is a complex of G. $\therefore\ h_1 \in G$.

Similarly $h_2 \in H_2 \Rightarrow h_2 \in G$.

$$\therefore\ h_1\,h_2 \in G.$$

Hence every element of $H_1\,H_2$ is an element of G.

$$\therefore \quad H_1 H_2 \subseteq G.$$

Therefore $H_1 H_2$ is also a complex of G (not a sub group).

(b) Multiplication of complexes is associative.

i.e. $H_1 (H_2 H_3 = (H_1 H_2) H_3,$

Let $h_1 \in H_1, h_2 \in H_2, h_3 \in H_3.$

$\therefore$ h_1, h_2, h_3 also belong to G, then

$$h_2 h_3 \in H_2 H_3, h_1 \in H_1.$$

$\therefore$ $h_1 (h_2 h_3) \in H_1 (H_2 H_3).$

Similarly $(h_1 h_2) h_3 \in (H_1 H_2) H_3.$

But as h_1, h_2, h_3 are elements of H in which the composition is associative.

$$\therefore \quad h_1 (h_2 h_3) = (h_1 h_2) h_3$$

Hence $H_1 (H_2 H_3)$ and $(H_1 H_2) H_3$ consist of the same elements. $\therefore$ $H_1 (H_2 H_3) = (H_1 H_2) H_3.$

(c) Inverse of a complex.

If H be a complex of H then the inverse of the complex of H is the set consisting of the inverses of the elements of H and is denoted by H^{-1}.

$$\therefore \quad H^{-1} = \{h^{-1} : h \in H\}.$$

(d) Inverse of the product of two complexes.

$$(H_1 H_2)^{-1} = H_2^{-1} H_1^{-1}$$

$$H_1 H_2 = \{h_1 h_2 : h_1 \in H_1, h_2 \in H_2\}.$$

$\therefore$ $(H_1 H_2)^{-1} = \{(h_1 h_2)^{-1} : h_1 \in H_1, h_2 \in H_2\}.$

But $h_1 \in H_1 \Rightarrow h_1 \in G$, $h_2 \in H_2 \Rightarrow h_2 \in G.$

$\therefore$ $(h_1 h_2)^{-1} = h_2^{-1} h_1^{-1}.$

$\therefore$ $(H_1 H_2)^{-1} = \{h_2^{-1} h_1^{-1} : h_1 \in H_1, h_2 \in H_2\}.$

$= (H_2)^{-1} (H_1)^{-1}$ by definition of multiplication of two complexes.

Theorem 6. *If H is a sub group of G then $H^{-1} = H$ but the converse is not true.*

Since H is a sub group. $\therefore \quad h \in H \Rightarrow h^{-1} \in H$

$\Rightarrow (h^{-1})^{-1} \in H^{-1} \Rightarrow h \in H^{-1}$

$\therefore \quad H \subseteq H^{-1}$. ...(1)

Again $h^{-1} \in H^{-1} \Rightarrow h \in H \Rightarrow h^{-1} \in H$ as H is a sub group.

$\therefore \quad H^{-1} \subseteq H$. ...(2)

Hence form 1) and (2) we get $H^{-1}=H$.

Converse. Let $G=\{1, -1, \times\}$ and $H=\{-1\}$ be a complex of G.

Now $(-1)^{-1}=-1 \quad \therefore \quad H^{-1}=\{-1\}=H$ but $\{-1\}$ *i.e.* H is not a sub group of G. Hence the converse is **not** true

Theorem 7 *The necessary and sufficient condition for a non empty sub set H i.e. a complex H of a group G to be a sub group is that* $H H^{-1} \subseteq H$.

Hence deduce that the above necessary and sufficient condition can also be written as $H H^{-1}=H$.

Necessary : Given. H is a sub group.

To prove. $H H^{-1} \subseteq H$.

Let $x \in HH^{-1} \Rightarrow x=ab^{-1}$ for some $a, b \in H$

$\Rightarrow x \in H$ because H is given to be a sub group and we know from Th. 2 P. 132. that $a, b \in H \Rightarrow ab^{-1} \in H$, where H is a sub group.

Hence $HH^{-1} \subseteq H$.

Sufficient : Given. $H H^{-1} \subseteq H$.

To prove that H is a sub group

Let $a \in H, b \in H$ then $ab^{-1} \in H H^{-1} \Rightarrow ab^{-1} \in H$

as $H H^{-1} \subseteq H$.

Since $a \in H, b \in H \Rightarrow ab^{-1} \in H$ therefore H is a ub group by theorem 2 P. 132.

2nd art.

Sufficient : Given. H is a sub group.

To prove. $H H^{-1}=H$.

Since H is a sub group. $\therefore$ $H H^{-1} \subseteq H$ by 1st part.

Again let $a \in H$ then $a=ae=ae^{-1} \in H H^{-1}$

$\therefore$ $H \subseteq H H^{-1}$

Hence $H=H H^{-1}$.

Necessary : Given. $H=H H^{-1}$.

To prove. H is a sub group.

Since $H=H H^{-1}$. $\therefore$ $H H^{-1} \subseteq H$ and hence by part 1 H is a sub group.

Theorem 8. *If H and K be two sub groups of a group G then $H K$ is a sub group if and only if $HK=KH$.*

(Agra M.Sc. 69; Meerut M.Sc B.Sc. 69)

Necessary : Given. $H K$ is a sub group.

To prove $H K=K H$.

Since H and K are sub groups.

$\therefore$ $H^{-1}=H, K^{-1}=K$. Th. 6. .. (1)

Again $H K$ is a sub group. $\therefore$ $(H K)^{-1}=H K$

or $K^{-1} H^{-1}=H K$ or $K H=H K$ by (1)

Sufficient : Given $H K=K H$.

To prove that $H K$ is a sub group.

By 2nd part of theorem 7 $H K$ is a sub group if

$(H K)(H K)^{-1}=H K$. ...(1)

Since H and K are sub groups.

$\therefore$ $H H^{-1}=H, K K^{-1}=K$. .. (2)

Now $(H\,K)\,(H\,K)^{-1}=(H\,K)\,(K^{-1}\,H^{-1})=H(KK^{-1})\,H^{-1}$

$=(H\,K)\,H^{-1}$ by (2) $=(K\,H)\,H^{-1}$

$\because\quad H\,K=K\,H$

$=K\,(H\,H^{-1})=K\,H$ by (2) ...(3)

But $K\,H$ is given to be $H\,K$.

$\therefore\quad (H\,K)\,(H\,K)^{-1}=H\,K$ and hence $H\,K$ is a sub group.

Deduction. *If H and K are sub groups of an abelian group G then HK is a sub group of G.*

As H and K are sub groups then we have

$$\left.\begin{aligned} H&=H^{-1},\ H\,H^{-1}=H\\ K&=K^{-1},\ K\,K^{-1}=K\end{aligned}\right\}\ \text{Th. 6 \& Th. 7}\qquad ...(A)$$

Also G is given to be abelian and hence $H\,K=K\,H$ ...(B)

Now $H\,K$ will be a sub group if we establish that

$$(H\,K)\,(H\,K)^{-1}=H\,K$$

We have already proved this relation above in Th. 8 by the help of conditions A and B.

§ 7. Sub groups of a cyclic group.

Theorem 9. *A sub group H of a cyclic group is also cyclic and is generated by a^m where a is a generator of G and m is least +ive integer such that $a^m \in H$.*

(Bombay M. Sc. 70; Lucknow 66, 68; Meerut 68, 70; Pb. 65, 70; Raj. M. Sc. 69; Utkal 69)

Let $G=\{a\}$ *i.e.*, a cyclic group generated by a then the sub group H of G will contain integral powers of a like a^s and also its inverse a^{-s} as H is a sub group. We have to show that H is cyclic and is generated by a^m where m is the least + ive integer such that $a^m \in H$. In other words we have got to show that H contains elements of the type $(a^m)^s$.

Let $a^s \in H$ where $s > m$.

$\therefore\quad s=mq+r$ where $0 \leqslant r < m$

$\therefore\quad a^s=a^{mq+r}=a^{mq}.a^r$.

Now $(a^m)^q \in H$ and hence its inverse $a^{-mq} \in H$ as H is a sub group.

Now $a^s \in H$ by supposition and $a^{-mq} \in H$.

$\therefore \quad a^s.a^{-mq} \in H$ or $a^{s-mq} \in H$ or $a^r \in H$.

$\because \quad s=mq+r$.

But r is less then m and hence it contradicts the fact that m is the least +ive integer such that $a^m \in H$.

Therefore $r=0$ and hence $s=mq$.

$\therefore \quad a^s=a^{mq}=(a^m)^q$.

Therefore every element a^s of the sub group H is of the form $(a^m)^q$ and hence H is generated by a^m *i.e.*, $H=\{a^m\}$.

Theorem 10. *If the order of a is zero i.e., G is an infinite cyclic group, then every proper sub group H of G is infinite except $\{e\}$.*

Let H be a sub group of an infinite cyclic group $G=\{a\}$ then H is again a cyclic group being generated by a^m *i.e.*, $H=\{a^m\}$ by *Th.* 9, where m is the least +ive integer such that $a^m \in H$. We have to prove that H is infinite. Let us suppose that H is finite. Also since $H \neq \{e\}$ we can assume that $m > 0$.

Since H is supposed to be finite and it is being generated by a^m

$\therefore \quad (a^m)^s=e$ for some $s > 0$

or $a^{ms}=e$

From this we conclude that a is of finite order or in other words it implies that G is finite which contradicts that G is infinite.

Theorem 11. *Every sub group of a finite cyclic group of order n is a finite cyclic group of order $\frac{n}{m}$ where a^m is the generator of sub group.*

Since the group G is finite and hence the order of a is $n > 0$ such that $a^n = e$ $\therefore$ $a^n \in H$ as $e \in H$. Since H is a sub group generated by a^m (theorem 9) and let its order be q so that $(a^m)^q = e = a^n$.

$$\therefore \quad a^{mq} = a^n \Rightarrow mq = n \Rightarrow q = \frac{n}{m}$$

Hence the sub group H consists of q elements a^m, $a^{2m} \ldots\ldots a^{mq}$ where $q = \frac{n}{m}$

Ex. *Let* $G = \{\omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6 = e\}$. *It is of order 6. Its proper sub groups are*

$$H_1 = \{\omega^2, \omega^4, \omega^6 = e\}.$$

The sub group H_1 is generated by ω^2 *i.e.*, $m = 2$ and its order is $\frac{n}{m} = \frac{6}{2} = 3$ *i.e.*, contains three elements.

Again $H_2 = \{\omega^3, \omega^6 = e\}$.

The sub group H_2 is generated by ω^3 *i.e.*, $m = 3$ and its order is $\frac{n}{m}$ *i.e.*, $\frac{6}{3} = 2$, *i.e.* it contains two elements,

§ 8. Cosets.

Definition. Let $H = \{h_1, h_2, \ldots\ldots, h_n\}$ be a sub group of a group G and a be any element of G then the set. $\{h_1 a, h_2 a, \ldots\ldots, h_n a\}$ denoted by Ha is called the **right coset** generated by a *i.e.*, $Ha = \{ha : h \in H\}$ and the set $\{ah_1, ah_2, \ldots\ldots, ah_n\}$ denoted by aH is called the left coset generated by a *i.e.*, $aH = \{ah : h \in H\}$ **(Lucknow 69)**

In additive notation.

right coset $= H + a = \{h + a : h \in H\}$

left coset $= a + H = \{a + h : h \in H\}$.

Note. In case G be abelian then right coset = left coset.

Exercise 2

Ex. I. *Let G be the symmetric group of permutations on four symbols a, b, c, d and let the sub group.*

$$H=\{I, (ab), (cd), (ab)\ (cd)\}$$

Choose $x \in G$ as $(a\ \ d\ \ c\ \ b)$ then the right coset

$Hx=\{hx : h \in H\}$

$=\{I\ o\ (a\ \ d\ \ c\ \ b), (ab)\ o\ (a\ \ d\ \ c\ \ b),$

$(cd)\ o\ (a\ \ d\ \ c\ \ b), (ab)\ (cd)\ o\ (a\ \ d\ \ c\ \ b)\}$

$=\{(a\ \ b\ \ c\ \ d), (bdc), (adb), (bd)\}$ ...(1)

$\because\ (ab)\ o\ (adcb)=\begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} o \begin{pmatrix} a & d & c & b \\ d & c & b & a \end{pmatrix}$

$=\begin{pmatrix} a & b & c & d \\ b & a & c & d \end{pmatrix} o \begin{pmatrix} b & a & c & d \\ a & d & b & c \end{pmatrix}=\begin{pmatrix} a & b & c & d \\ a & d & b & c \end{pmatrix}$

$=\begin{pmatrix} a & b & d & c \\ a & d & c & b \end{pmatrix}=(\ b\ \ \ d\ \ \ c\ )$ etc

Similarly the left coset,

$xH=\{xh : h \in H\}$

$=\{(a\ d\ c\ b)\ o\ I, (a\ d\ c\ b)\ o\ (a\ b), (a\ d\ c\ b)\ o\ (c\ d),$

$(a\ d\ c\ b)\ o\ (a\ b)\ (c\ d)\}$

$=\{(a\ d\ c\ b), (a\ d\ c), (a\ c\ b), (a\ c)\}.$ ...(2)

From *I* and 2 we observe that $Hx \neq xH$.

Ex. 2. *Prove that H itself is a right coset as well as left coset.*

We know that the identity element e of G is also the identity element of sub group H. Hence choosing $a=e$ we have

Right Coset $He=\{h\ e : h \in H\}=\{h : h \in H\}$

$\because\ he=h\ \forall\ h \in H.$

$$H\ e=H$$

or

Left Coset $e\ H=\{e\ h : h \in H\}=\{h : h \in H\}$

$\because\ e\ h=h\ \forall\ h \in H$

$$e\ H=H$$

or

$\therefore$ Hence H is a right as well as a left Coset.

Ex. 3. *Prove that* $a \in a\,H$ *and* $a \in H\,a$

$$a\,H=\{a\,h : h \in H\}.$$

Since $e \in H$ therefore one of the h^s must be e and hence the set $a\,H$ contains a

$$\because \quad a\,h=a\,e=a, \text{ Also } h\,a=e\,a=a$$

$$a \in a\,H. \text{ and } a \in H\,a$$

Hence both the left and right cosets $a\,H$ and $H\,a$ are non empty as at least the element a belongs to both of them.

Ex. 4. *Let* $G=\{\ldots -4, -3, -2, -1, 0, 1, 2, 3, 4\ldots)+$

$H=$ Sub group consisting of multiples of a given integer say 3, *i e.*

$H=\{\ -9, -6, -3, 0, 3, 6, 9\ldots\}+$

To show that $G=H \cup (H+1) \cup (H+2)$.

We know that $H+0=H=\{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}$

The Coset $H+1=\{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}$

The Coset $H+2=\{\ldots, -7, -4. -1, 2, 5, 8, 11, \ldots\}$.

The Cost $H+3=\{\ldots -6, -3, 0, 3, 6, 9, 12, \ldots\}$

and it is same as $H+0$

Similarly $H+4$, Coset is same as Coset $H+1$, $H+5$ is same as $H+2$ and so on.

Thus there are only three distinct Cosets

$$H,\ H+1,\ H+2$$

and

$$G=H \cup (H+1) \cup (H+2).$$

Ex. 5. $G=\{a, a^2, a^3, a^4=I\} \quad o\,(G)=4$

$H=\{1, a^2\}$ *is a sub group of* G

Find all the cosets of H *in* G *and prove that* G *is equal to union of all these cosets and also establish that any two cosets are either disjoint or identical*

$$1.H=\{1, a^2\}=H$$

$$a.H=\{a, a^3\}$$

$$a^2 . H=\{a^2, a^4\}=\{a^2, 1\}=H$$
$$a^3 . H=\{a^3, a^5\}=\{a^3, a\}=\{a, a^3\}=a . H \quad \because \quad a^4=1$$

Thus there are only two distinct cosets namely H and $a\,H$ which are disjoint. Also H is identical with $a^2\,H$ and $a\,H$ is identical with $a^3\,H$

Again $H \cup a\,H=\{1, a^2\} \cup \{a, a^3\}=\{1, a, a^2, a^3\}=G$

§ 9. Theorem on Cosets.

Theorem 12. *If h belongs to sub group H of G, then*

$$h\,H=Hh=H.$$

i e. right and left Cosets corresponding to any element $h \in H$ are H.

$$H=(h_1, h_2, \ldots h_i \ldots)$$
$$hH=(h\,h_1, h\,h_2, \ldots h\,h_i, ..) \text{ where } h \in H.$$

Since H is a sub group.

$$\therefore \quad h \in H, h_i \in H \Rightarrow h\,h_i \in H \;\forall\; i.$$

Thus all the elements of $h\,H$ are again elements of H.

$$\therefore \quad h\,H \subset H. \qquad \ldots(1)$$

Now we shall show that any element h_i of H is an element of $h\,H$ which would imply $H \subset h\,H$. . (2)

From (1) and (2) we shall prove that $h\,H=H$.

Now choose h_i any arbitrary element of H

$$h_i=e\,h_i=(h\,h^{-1})\,h_i=h\,(h^{-1}\,h_i) \in h\,H.$$
$$\because \quad h \in H, \quad \therefore \quad h^{-1} \in H, h_i \in H, \quad \therefore \quad h^{-1}\,h_i \in H.$$
$$\therefore \quad H \subset h\,H \text{ etc.}$$

In order to prove $H\,h=H$, we shall establish as above that

$$H\,h \subset H,$$

and then $h_i=h_i e=h_i\,(h^{-1}\,h)=(h_i\,h^{-1})\,h \in H\,h.$

$$\because \quad h \in H, \quad \therefore \quad h^{-1} \in H, h_i \in H, \quad \therefore \quad h_i\,h^{-1} \in H$$
$$\therefore \quad H \subset H\,h \text{ and hence } H=H\,h.$$

Theorem 13. *H is a sub group of a group G and a is any arbitrary element of G, prove that*

$$Ha=H \Leftrightarrow a \in H$$
$$a\,H=H \Leftrightarrow a \in H$$

Ist Case. $Ha=H$ ...(1)

to show $a \in H$

$e \in H, a \in H \quad \therefore \quad ea \in Ha$

or $a \in Ha$ or $a \in H$ by (1)

Converse. $a \in H$ ...(2)

to show that $Ha=H$

Let $x \in Ha \Rightarrow x=ha$ where $h \in H$ and $a \in H$ (given)

Since H is a sub group therefore

$$h \in H, a \in H \Rightarrow ha \in H$$

Hence $x \in Ha \Rightarrow x=ha \in H \quad \therefore \quad Ha \subset H$ ...(3)

Again let $y \in H$ then $y=ya^{-1}a \quad \because \quad a^{-1}a=e$

or $$y=(ya^{-1})a$$

Now $a \in H \Rightarrow a^{-1} \in H$ as H is a sub group.

Also $y \in H, a^{-1} \in H \Rightarrow ya^{-1} \in H$

$\therefore \quad y=(ya^{-1})a \in Ha$

$\therefore \quad H \subset Ha$ ...(4)

Hence from (3) and (4) we get $H=Ha$

Similarly we can prove the other part.

Theorem 14. *Any two right (left) cosets of a sub group H of G are either disjoint or identical.*

Let $H=\{h_1, h_2, h_3, \ldots\}$ and $a, b \in G$, then

$$Ha=\{h_1a, h_2a, h_3a, \ldots\}$$

and $$Hb=\{h_1b, h_2b, h_3b, \ldots\}$$

are two right Cosets.

Let us suppose that Ha and Hb have some elements common and with that supposition we shall prove that all the elements in Ha and Hb are common. This will establish that either they are identical or they are disjoint, *i,e.* either $Ha \cap Hb=\phi$ *i.e.* disjoint or $Ha=Hb$

Let $h_1 a = h_2 b$ be the common elements of the two Cosets.

$$\therefore \quad h_2^{-1} h_1 \; a = h_2^{-1} h_2 \; b = e \; b = b.$$

Now $h_1 \in H$, $h_2^{-1} \in H$. $\therefore$ $h_2^{-1} h_1 \in H$ as it is a sub group.

Let $h_2^{-1} h_1$ be h_t.

$\therefore$ $h_t \, a = b$. Take cosets of both sides.

$\therefore$ $H (h_t \, a) = H \, b$ or $(H \, h_t) \, a = H \, b$ ...(1)

But $h_t \in H$ $\therefore$ $(H \, h_t) = H$ by Theorem 12.

$\therefore$ $Ha = Hb$. by (1)

Hence the two right Cosets are identical if they have some elements in common or else they are disjoint.

Similarly by taking $a \, h_1 = b \, h_2$ we get $a = b \, h_2 \, h_1^{-1} = b \, h_t$ say or $aH = (b \, h_t) \, H$ or $a \, H = b \, (h_t \, H) = b \, H$,

$\because$ $h_t \, H = H$ when $h_t \in H$.

We can prove that left cosets are either identical or disjont.

Deduction. *The only right or (left) coset of a sub group H of G which is also a sub group of G is H itself.*

H a is a right coset and if it is a sub group then e $\in$ *H a. But e* $\in$ *H which is a sub group as well as a right coset by Ex. 2. Thus e is common to both right cosets H and H a. But right cosets are either disjoint or identical (Th. 14).*

$$\therefore \quad H \, a = H.$$

Cor. I, If the elements $a, b, c, \ldots$ of G be so chosen that the cosets $H \, a$, $H \, b$, $H \, c$, .. are all disjoint then

$$G = H \cup H \, a \cup H \, b \cup H \, c, \ldots$$

H being the coset corresponding to identity element

or $$G = H \cup a \, H \cup b \, H \cup c \, H, \ldots$$

Theorem 15. *If a, b are any two distinct elements of G, then*

$$H \, a = H \, b \Leftrightarrow ab^{-1} \in H$$

$$a \, H = b \, H \Leftrightarrow b^{-1} a \in H$$

Let $H a = H b$, $\therefore$ $H a b^{-1} = H b b^{-1} = H e = H$.
But $H h = H$ only when $h \in H$ Theorem 12.
Hence $a b^{-1} \in H$,
Conversely. $a b^{-1} \in H$. To prove that $H a = Hb$.
Since $a b^{-1} \in H$, $\therefore$ $H a b^{-1} = H$,
$\because$ $H h = H$ when $h \in H$.
$\therefore$ $H a b^{-1} b = H b$ or $Ha = Hb$.

Left Cosets. $a H = b H$,
$\therefore$ $b^{-1} a H = b^{-1} b H = e H = H$.
But $h H = H$ only when $h \in H$. $\therefore$ $b^{-1} a \in H$.
Conversely $b^{-1} a \in H$. $\therefore$ $b^{-1} a H = H$,
$\because$ $h H = H$, when $h \in H$
or $b b^{-1} a H = b H$ or $a H = b H$

Exercise 3

1. *It a and b are any two distinct elements of a group G and H is any sub group of G then*

$$a \in H b \Leftrightarrow H a = H b$$

and $$a \in b H \Leftrightarrow a H = b H$$

Let $a \in H b$ $\therefore$ $ab^{-1} \in H bb^{-1}$
or $a b^{-1} \in He$ or $a b^{-1} \in H$.
$\therefore$ $H a b^{-1} = H$ $\because$ $h \in H \Rightarrow H h = H$ Th. 12.
or $H a b^{-1} b = H b$
or $H a e = H b$ or $H a = H b$ proved.

Converse. Let $H a = H b$

But we know that $a \in H a$ and since $H a = H b$ and hence it follows that $a \in H b$

In a similar manner we can prove the other part.

2. *Prove that the two right cosets H a, H b are distinct if and only if the two left cosets $a^{-1} H$, $b^{-1} H$ are distinct.*

Let $H a$, $H b$ be distinct then we have to show that $a^{-1} H$, $b^{-1} H$ are also distinct, If they are not distinct then they are identical. (Theorem 14).

$\therefore$ $a^{-1} H = b^{-1} H \Rightarrow$ there exist $h_i, h_j \in H$, such that $a^{-1} h_i = b^{-1} h_j$)

$\Rightarrow a\, a^{-1} h_i = a\, b^{-1} h_j \Rightarrow h_i = a\, b^{-1} h_j$

$\Rightarrow h_i\, h_j^{-1} = a\, b^{-1}$

$\Rightarrow H(h_i\, h_j^{-1}) = H(a\, b^{-1})$

But $h_i\, h_j^{-1} \in H$ and $H\, h = H$ when $h \in H$.

$\Rightarrow H = H\, a\, b^{-1}$

$\Rightarrow ab^{-1} \in H$ as above,

$\Rightarrow H\, a = H\, b$, (A)

[by Theorem 15, *i.e.* $H\, a = H\, b \Leftrightarrow a\, b^{-1} \in H$
$a\, H = b\, H \Leftrightarrow b^{-1} a \in H$.]

Result (A) is a contradiction to the supposition that $H\, a$ and $H\, b$are distinct. Therefore $a^{-1} H$, $b^{-1} H$ should be distinct.

Converse. Let $a^{-1} H$, $b^{-1} H$ be distinct then we have to show that $H\, a$ and $H\, b$ are distinct. If they are not distinct then they are identical, $\therefore$ $H\, a = H\, b \Rightarrow$ that there exists $h_i, h_j \in H$,

such that $h_i\, a = h_j\, b$.

$\Rightarrow h_i\, a\, a^{-1} = h_j\, b\, a^{-1} \Rightarrow h_i = h_j\, b\, a^{-1}$

$\Rightarrow h_j^{-1} h_i = h_j^{-1} h_j\, b\, a^{-1} = b\, a^{-1}$

$\Rightarrow (h_j^{-1} h_i)\, H = (b\, a^{-1})\, H$ but $h_j^{-1} h_i \in H$

$\Rightarrow H = b\, a^{-1} H$ $\quad\because\quad hH = H$ when $h \in H$

$\Rightarrow b\, a^{-1} \in H$

$\Rightarrow (b^{-1})^{-1} a^{-1} \in H$

$\Rightarrow a^{-1} H = b^{-1} H$,

by Theorem 15, *i.e.* $a\, H = b\, H \Leftrightarrow b^{-1} a \in H$

or $a^{-1} H = a^{-1} H \Leftrightarrow (b^{-1})^{-1} a^{-1} \in H$,

which is a contradiction to the supposition that $a^{-1} H$ and $b^{-1} H$ are distinct. Hence *Ha*, *Hb* are distinct.

3. *Prove that the set of the inverses of the elements of a right coset is a left coset i.e.* $(Ha)^{-1} = a^{-1} H$

Let H be a sub group of group G and $a \in G$ then the right coset

$H\,a=\{h_1\,a,\ h_2\,a\ ..h_i\,a...\}$

$(Ha)^{-1}=\{(h_1\,a)^{-1},\ (h_2,\ a)^{-1},.....\}=A$

$a^{-1}H=\{a^{-1}\,h_1,\ a^{-1}\,h_2,.....\}=B$

Any element of A *i e.* $(H\,a)^{-1}$ is $(h_i a)^{-1}=a^{-1}\,h_i^{-1}=a^{-1}\,h_j$ say

But $a^{-1}\,h_j$ is an element of left coset $a^{-1}\,H$ *i.e.* B.

$\therefore \quad A \subset B$ ...(1)

Again any element of B *i.e.* $a^{-1}\,H$ *i.e.* $a^{-1}\,h_i=a^{-1}\,(h_i^{-1})^{-1}$

$=(h_i^{-1}\,a)^{-1}=(h_j\,a)^{-1}$ say

Since $h_j\,a \in H\,a \quad \therefore \quad (h_j\,a)^{-1} \in (H\,a)^{-1}=A$

$\therefore \quad B \subset A$ ...(2)

Hence from (1) and (2) we get $A=B$ or $(H\ a)^{-1}=a^{-1}H$.

4. *Given that* $G=H \cup H\,a_1 \cup H\,a_2 \cup ..\cup Ha_k$ *is the right coset decomposition of* G *relative to sub group* H *show that* $G=H \cup a_1^{-1}\,H \cup a_2^{-1}\,H \cup ...\cup a_k^{-1}\,H$ *is a left coset decomposition of* G *relative to the sub group* H.

We have proved in Ex. 3. that $(Ha)^{-1}=a^{-1}\,H$

Then $a^{-1}\,H$ is a left coset consisting of the inverses of the elements of the right c. set Ha. Hence corresponding to each right coset Ha_k we have a left cosel $a_k^{-1}\,H$. Therefore

$$G=H \cup a_1^{-1}\,H \cup a_2^{-1}\,H \cup ...\cup a_k^{-1}\,H$$

is a left coset decomposition of G relative to H.

Theorem 16. *If* H *be a sub group of the group* G, *prove that the number of left cosets of* H *in* G *is equal to the number of right cosets of* H *in* G. **(Benares B. Sc. 67)**

Here we shall prove that corresponding to each left coset we have a right coset and if two left cosets are identical then the corresponding right cosets are also identical.

We know that $a\,H$ is a left coset

and $a \in a\,H$, and $b \in b\,H$

and if $a, b \in$ to same left coset then $a\,H = b\,H$. Because the two left cosets are either identical or distinct.

But $a\,H = bH \Leftrightarrow b^{-1}a \in H$ Theorem 15,P.155 .. (1)

Similarly if $a, b \in$ same right coset then

$$H\,a = H\,b \Leftrightarrow a\,b^{-1} \in H. \quad .. (2)$$

Now let us define a mapping $f : G \to G$, such that

$$f(a) = a^{-1},\ a \in G$$

f is a one-one mapping of G onto itself as inverse of each element exists and is unique.

Now if a, b belong to the same left coset then by (1) $b^{-1}a \in H$.

This relation can be written as $(b^{-1})\,(a^{-1})^{-1} \in H$,

From this we get $Hb^{-1} = H\,a^{-1}$ by (2)

Therefore a^{-1} and b^{-1} belong to the same right coset of H in G.

Thus we observe that if a, b belong to the same left coset then their images under the mapping f belong to the same right coset of H in G.

Therefore the mapping f induces a one-one correspondence

$$a\,H \to H\,a^{-1}$$

between the set of left cosets of H in G and the set of right cosets of H in G.

Hence **proved.**

Theorem 17. *The mapping f defined by $f(a\,H) = H\,a^{-1}$ is one-one mapping from the set of all left cosets of H in G onto the set of all right cosets of H in G.*

Let us first establish that the given mapping is well defined. Now if $a\,H$ is a left coset then $H\,a^{-1}$ is right coset. Now if $a\,H$ and $b\,H$ represent the same left coset then we have to show that $f(a\,H) = f(b\,H)$ or $H\,a^{-1} = Hb^{-1}$

Now $a\,H=b\,H \Rightarrow b^{-1}a \in H$ Th. 15 P. 155

$H\,b^{-1}\,a=H$ $\because$ $Hh=H$ if $h \in H$

$\Rightarrow H\,b^{-1}\,a\,a^{-1}=H\,a^{-1} \Rightarrow H\,b^{-1}=H\,a^{-1}$

i e. $f(bH)=f(aH)$

In order to establish that the **mapping is one-one** we shall show that

$f(a\,H)=f(bH) \Rightarrow a\,H=b\,H.$

Now $f(a\,H)=f(b\,H) \Rightarrow H\,a^{-1}=H\,b^{-1}$

$\Rightarrow a^{-1}\ (b^{-1})^{-1} \in H$ Th. 15 *i.e.* $H\,a=H\,b \Rightarrow a\,b^{-1} \in H$

$\Rightarrow a^{-1}b \in H.$

$\Rightarrow a\,a^{-1}\,b \in a\,H \Rightarrow b \in a\,H.$

But b also belongs to $b\,H$ as H is a group and e is its element $\therefore$ $b\,e=b$ is an element of $b\,H$.

Hence b belongs to both bH and aH, But we know that two left cosets bH and aH are either disjoint or identical. Since they have a common element and as such they are identical

$\therefore$ $b\,H=a\,H$ **Proved.**

For onto. Let $H\,a$ be any right coset then $a^{-1}\,H$ is a left coset

Also $f(a^{-1}\,H)=H\,(a^{-1})^{-1}=Ha$ by def. of f

Thus each right coset Ha is the f image of the left coset $a^{-1}\,H$ and hence the function f is **onto.**

Ex 1. *If H is a sub group of G then there exists a one-one correspondence between any two right cosets of H in G. i.e their exists a bijection from Ha to Hb.*

Let Ha and Hb he any two right cosets of H in G.

so that $h\,a \in Ha$, $hb \in Hb\ \forall\ h \in H$. Let us define a mapping $f : Ha \to Hb$ such that

$f(ha)=hb.$

The mapping is one-one. $f(h_1\,a)=f(h_2\,a) \Rightarrow h_1\,b=h_2\,b.$

$\Rightarrow h_1=h_2$ by cancellation law

$\Rightarrow h_1\,a=h_2\,a$ $\therefore$ f is one-one.

Clearly the mapping is onto because for each element h_1b

in Hb there exists an element $h_i a$ in Ha. Hence the mapping f is a bijection.

Ex. 2. *Prove that there exists a one-one-correspondence between H and aH*

Let $f : H \to a\,H$ *defined as* $f(h)=ah \;\forall\; h \in H$.

f is one-one ; $f(h_i)=f(h_j) \Leftrightarrow ah_i=ah_j \Leftrightarrow h_i=h_j$ by cancellation law.

f is onto : Corresponding to each $ah_i \in aH$ there exists h_i in H such that $f(h_i)= a\,h_i$.

Hence the mapping f is **a bijection.**

§ 10. Coset Decomposition.

From theorem 14 we observe that the two right (left) cesets of a sub-group H in G are either disjoint or identical. Hence the set of all right (left) cosets of a sub group H gives a decomposition of G into mutually disjoint classes.

Congruence relation.

Let H be a sub group of a group G and a, b be any two elements of G then we define a congruence relation in G experessed as

$$a \equiv b \ (Mod\ H).$$

i e. a is congruent to b modulo H if and only if $a\,b^{-1} \in H$.

We may recall from theorem 15 P.155 that

$$Ha = Hb \Rightarrow ab^{-1} \in H$$

Theorem 18. *To prove that the relation of congruency modulo H is an equivalence relation.* **(Meerut M. Sc. 68; Luck. 69; Agra 70; Utkal 70; B H. U. 70)**

In order to prove that the relation $a \equiv b$ (Mod. H) is an equivalence relation we have to establish that it is reflexive, symmetric and transitive.

From definition $a \equiv b$ (Mod. H) if $a\,b^{-1} \in H$.

Reflexive. $a \equiv a$ Mod. H) if $a\,a^{-1} \in H$

which is ture as H is a sub group. Hence reflexive.

Symmetric. $a \equiv b$ (Mod. H) $\Rightarrow a\,b^{-1} \in H$.

Since H is a sub group and $a\,b^{-1} \in H$

$$\therefore \quad (a\,b^{-1})^{-1} \in H.$$

or $$(b^{-1})^{-1}\,a^{-1} \in H \text{ or } b\,a^{-1} \in H.$$

$$\therefore \quad b \equiv a \text{ (Mod. } H\text{) by definition.}$$

Hence Symmetric.

Transitive. $a \equiv b$ (Mod. H), $b \equiv c$ (Mod. H)

i.e. $$a\,b^{-1} \in H \text{ and } b\,c^{-1} \in H.$$

Since $a\,b^{-1}$ and $b\,c^{-1} \in H$ and H is a sub group.

$$\therefore \quad (a\,b^{-1})\,(b\,c^{-1}) \in H$$

$$a\,(b^{-1}\,b)\,c^{-1} \in H$$

$$a\,(e)\,c^{-1} \in H.$$

$$a\,c^{-1} \in H \quad \therefore \quad a \equiv c \text{ (Mod. } H\text{).}$$

Hence transitive.

Therefore the congruency relation is an equivalence relation and it decomposes the group G into disjoint equivalence classes which are the right cosets of H in G. In order to obtain such disjoint right cosets we proceed as below.

H is a right coset of H in G.

Now if a does not belong to H then it belongs to Ha.

$$\because \quad a = e\,a \in Ha \quad \text{as} \quad e \in H.$$

Next if b does not belong to H or Ha then the next right coset is Hb and so on.

In this way we obtain the disjoint right cosets as

$$H, Ha, Hb, Hc, \ldots\ldots$$

It may be shown as above that the relation $b^{-1}a \in H$ is an equivalence relation in G

$$[b^{-1}a \in H \Leftrightarrow aH = bH, \text{ Th. 14}]$$

such that the corresponding equivalence classes coincides with the set of the left cosests of H in G.

Index of H in G. The number of distinct right (left)

cosets of H in G is called the index of H in G and is denoted as $[G : H]$. **(Punjab 66)**

§ 11. Lagranges Theorem.

Statement *The order of a sub group H of a finite group G is a divisor of the order of the group G.*

(Gorakhpur 70; Luck 66, 68; Utkal 70; B H.U. 68; Allahabad 69; Rajasthan 69; Meerut M.Sc. 67 68; Raj. M.Sc. 69; Delhi 70; Pb. 66, 67, 69, 70)

Let the order of the finite group G be n and the order of its sub group H be m.

We consider the right coset decomposition of G relative to H

$$H=\{h_1, h_2, \ldots\ldots, h_m\},$$

$\therefore$ $Ha=\{h_1 a, h_2 a, \ldots\ldots, h_m a\}$ are the m members of the right coset Ha, where $a \in G$.

All the m elements of right coset Ha are distinct for if not then

$$h_i a=h_j a \Rightarrow h_i a a^{-1}=h_j a a^{-1} \Rightarrow h_i=h_j$$

which is not true. Hence all the members of the right coset Ha are distinct.

Again since the group G is finite the number of such right cosets will be finite. Let the number of disjoint right cosets be k. [It should be noted that the number of cosets will not be n the number of elements of G.

$$\because \quad a \in H \Rightarrow Ha=H \quad \forall \ a \in H$$

i e. all those members of G which are also members of H will give only one coset H. Also we know that the right cosets are either disjoint or identical. This explains for our taking the number of distinct right cosets to be k instead of n.

Again since all these right cosets are disjoint.

$$\therefore \quad G=H \cup Ha_1 \cup Ha_2 \ldots\ldots \cup Ha_k.$$

Hence the total number of elements of G=number of elements in the k cosets=mk, as each coset consists of m elements

$$\therefore \quad n=mk \quad \text{or} \quad m=\frac{n}{k} \qquad \ldots(1)$$

i.e. $$\text{order of } H=\frac{\text{order of } G}{K}$$

or order of sub group H *i.e.* m is the divisor of the order of the group G which is n.

Converse of Lagranges Theorem

The converse of Lagranges Theorem is not true *i.e.* if G be a group of order n and m is any divisor of n then it is not necessary that G may have a sub group of order m. we shall illustrate the same by an example.

S_4=Symmetric group of permutation on 4 symbols consisting of 4 !=24 elements.

A_4=Alternative group consisting of even permutations which will be 12, so that its order is 12

But there is no sub group H of A_4 whose order is 6 even though 6 is a divisor of 12 the order of A_4.

Cor. 1. *The index k of a sub group H of a finite group G is a divisor of the order of G.* **(Raj. M.Sc. 67)**

Above is clear from (1) and the definition of index of a sub group *i.e.* $k=\frac{n}{m}$.

Cor. 2. *The order of an element of a finite group is a divisor of the order n of the group, In particular* $a^n=e$.

(Punjab 70; Meerut 70; B.H.U. 70; Poona 70; Luck. 67)

Let n be the order of a finite group G and $a \in G$ be its element whose order is m *i.e.* $a^m=e$, where m is the least +ive integer satisfying the above relation.

Consider the cyclic group

$$a, a^2, a^3, \ldots\ldots, a^m = e.$$

It is a sub group of G because

$$a \in H, b \in H \Rightarrow a\,b \in H,$$

by the help of $a^m = e$.

Also the order of this sub group is m.

Hence by Lagrange theorem $\left[m = \frac{n}{k}\right]$ order of a sub group *i.e.* m is a divisor of the order of G *i e.* n. Or order of an element a of a group G *i.e.* m is a divisor of the order of G *i.e.* n. Again $a^n = a^{mk} = (a^m)^k = e^k = e$.

Cor. 3. *If a finite group of order n contains an element of order n, then the group must be cyclic.*

Let $a \in G$ where G is a finite group of order n.

Also $o(a) = n$ (given)

Consider the cyclic sub group H of G which is generated by a *i.e.* $H = \{a^r : r \in I\}$

Clearly the order of H is n as the order of its generator is n.

Thus H is a cyclic sub group of G whose order is the same as that of G. Thus $H = G$ and because H is cyclic therefore G is also cyclic.

Cor. 4. *Every group of prime order p is cyclic.*

(Gorakhpur 70; Kanpur 69; Luck 66; Delhi Hons, 69; Raj. M.Sc. 67; Meerut B Sc. 70)

Let G be a group of order p where p is prime.

Let a be any element of G whose order is m *i.e.* $a^m = e$.

Consider the cyclic sub group H generated by a,

i.e. $H = \{a, a^2, a^3, \ldots\ldots, a^m = e\}$.

The order of this cyclic sub group *i.e.* m is a divisor of the order of the group G which is p and p is prime. This is possible only when $m=p$.

Hence the given group G of order p will consist of elements which will be powers of a, and hence it is cyclic. [Elements of sub group H are elements of G] and we have shown that $m=p$. Hence $H=G$ when $m=p$ and therefore G is a cyclic.

Cor 5. *Every finite group of composite order possesses proper Sub groups.* **(Meerut 70; Delhi Hon's 70)**

Let G be a finite group of composite order mn where $m\neq 1$, $n\neq 1$.

Case I : Suppose that G is Cyclic and a is a generator of G then clearly $o(a)=mn$ as order of G is mn

$$\therefore \quad o(a^n)=m.$$

Now consider the cyclic sub group $H=\{a^n\}$

The order of H is order of its generator which is m where $m\neq 1$ and $m<mn$. Hence H is a proper sub group, because if $m=1$ and $m=mn$,

then H would be improper sub group.

Case II. Let G be not-cyclic. In this case the order of each element of G must be less than mn. Hence G will contain at least one element say b of order p where $p\neq 1$ and $p<mn$. Hence $H=\{b\}$ is a sub group of G whose order is $p\neq 1$, $p < mn$,

Thus H is a proper sub group of G.

Cor 6. *A group G having no proper sub group must be a finite group of order n where n is either 1 or prime* **(Punjab 70)**

Let G be an infinite group and $a\neq e$ and $a \in G$

Case I. If $o(a)=$ finite, then $H=\{a\}$ *i.e* a cyclic group

generated by a is a proper sub group of G whose order is same as $o(a)$. But we are given that G has no proper sub group Hence G must be finite.

Case II. If $o(a)$=infinite then $\{a\}$ is a sub group of G. If $G=\{a\}$ then G is an infinite cyclic group and hence G must have proper sub groups. On the other hand if $G\neq\{a\}$ then $\{a\}$ is a proper sub group of G. But we are given that G has no proper sub group and hence G must be a finite group. Again the order of G must be prime or 1 for otherwise order of G will be composite and we know that every group of composite order has proper sub groups.

Theorem 19. *If $G=\{a\}$ be a finite cyclic group of order n then for any divisor d of n there exists a unique sub group of G of order d.*

Proof. Existence :

$G=\{a\}$ is a finite cyclic group of order $n \Rightarrow a^n=e$. .. (1)

Also d is a divisor of $n \Rightarrow n=dm$ for some m. .. (2)

From (1) and (2) we get

$$a^n=a^{dm}=(a^m)^d=e.$$

Hence order of $a^m \leqslant d$

Now let us suppose that s $(<d)$ is the order of a^m and hence $(a^m)^s=e$ or $a^{ms}=e$ where $ms < md$ or $<n$ by (1)

This is a contradiction to the fact that order of a is n *i.e.* $a^n=e$, and here we have shown that there exists $ms<n$ such that $a^{ms}=e$.

Therefore it follows that order of a^m cannot be less than d and it is equal to d.

Now $a^m \in G$ and order $a^m=d$, hence $\{a^m\}$ is a cyclic sub group of G of order d.

Uniqueness. Let us suppose that there is another sub group $\{a^k\}$ which is also of order d where $d=nm$.

We shall establish that $\{a^k\}=\{a^m\}$.

By division Algorithm there exists integers q and r such that $k=mq+r$ where $0 \leqslant r < m$.

$\therefore$ $kd=mqd+rd$ where $0 \leqslant rd < md$ *i.e.* n.

Now $a^{kd}=a^{mqd+rd}=a^{mqd}.a^{rd}=(a^{md})^q.a^{rd}$

or $a^{kd}=e^q.a^{rd}=a^{rd}$ $\because$ $md=n$ and $a^n=e$. .. (3)

But we have taken sub group $\{a^k\}$ to be of order d and hence its generator is of order d such that

$$(a^k)^d=e \quad i\,e. \quad a^{kd}=e,$$

Hence from (3) we get $e=a^{rd}$ where $rd < n$ and order of a is n *i.e.* $a^n=e$.

Above will not hold good unless $rd=0$ or $r=0$.

Putting $r=0$ in $k=mq+r$ we get $k=mq$

$\therefore$ $a^k=a^{mq}=(a^m)^q$. It follows that $a^k \in \{a^m\}$.

$\therefore$ $\{a^k\} \subseteq \{a^m\}$.

But the order of both the sub group, $\{a^k\}$ and $\{a^m\}$ was supposed to be d *i.e.* they have the same number of elements so the relation $\{a^k\} \subseteq \{a^m\}$ can be strengthened to $\{a^k\}=\{a^m\}$.

Theorem 20. *Prove that the index of every sub group of an infinite cyclic group is finite and thus to each positive integer m there corresponds one and only one sub group of index m.*

G is an infinite cyclic group and let H be its sub group then by theorem 10 *P.* 147 H is also infinite cyclic group being generated by a^m where m is the least +ive integer such that $a^m \in H$.

By index of a sub group we mean the number of distinct right cosets or left cosets

$H=\{a^m, a^{2m}, a^{3m}, ..,\}$ by def.

$Ha=\{a^{m+1}, a^{2m+1}, a^{3m+1}, ..,\}$

$Ha^2=\{a^{m+2}, a^{2m+2}, a^{3m+2}....,\}$

... ...

$Ha^{m-1}=\{a^{2m-1}, a^{3m-1}, a^{4m-1},.. ,\}$

Our assumption is that these are the only distinct right cosets because

$$Ha^m=\{a^{2m}, a^{3m},\ldots,\}$$

which has elements in common with H and hence $Ha^m=H$

Similarly $Ha^{-1}=\{a^{m-1}, a^{2m-1}, a^{3m-1},\ldots,\}$ which has elements in common with Ha^{m-1} and hence

$$Ha^{m-1}=Ha^{-1}$$

[any two right (left) cosets are either disjoint or identical].

Thus the number of distinct right cosets of H is m *i.e.* finite, also this decomposition for a given m is unique so that there is one and only one sub group of index m.

List of Important Questions and Articles.

Th. 1, 2 P. 131–132, Th 3 P. 134,
Exercise 1 P. (136-140) Q. (2, 3, 6) § 4 P. 140,
Th 8 P. 145, Th. 9 P. 146, Th. 14 P. 152
Th. 15 P. 153, Q. 2 P. 154, Th. 16 P. 156 Th. 18 P. 159
§ 11 P. 161 (V. Imp.) along with all its corollaries
Th. 19 P. 165.

CHAPTER III

RINGS

§ 1. In the last chapter we had defined group as a non empty set equipped with **one binary composition** and satisfying certain axioms. Here in this chapter we shall deal with an algebraic structure equipped **with two binary compositions** denoted additively and multiplicatively *i e.*, by $+$ and $.$ It will be known as Ring.

Definition : Ring. **(Meerut M. Sc. 67, B. Sc. 70; Lucknow 69; Marthwada 70; Raj. M. Sc. 67; Kanpur 69; Gujarat 70; Allahabad 67)**

A non empty set R with two binary compositions to be denoted additively and multiplicatively by symbols $+$ and $.$ is called a ring $(R,+,.)$ if it satisfies the following axioms.

R_1 *The set R is an abelian group for the additive composition.*

R_2 *Multiplication is a binary composition which is associative.*

R_3 *Multiplication is both right and left distributive with regard to addition.*

We shall refer as R_1, R_2 and R_3 the above axioms of a group which are explained as below.

R_1 **The set R is an abelian group for the addition composition.**

(1) **Closure property** *i.e.*, $a, b \in R \Rightarrow a+b \in R$.

This is implied because addition is a binary operation.

(2) **Associative** *i.e.*, $(a+b)+c=a+(b+c)\ \forall a, b, c \in R$

(3) **Identity** *i.e.*, $a+0=0+a=a\ \forall\ a \in R$

0 is called the additive identity.

(4) **Inverse.** For every element $a \in R$ there exists an element $b \in R$ such that $a+b=0$ (identity)$=b+a$.

Then b is called inverse of a. The inverse of any element a will be denoted by $(-a)$.

(5) **Commutative** *i.e.*, $a+b=b+a \ \forall \ a, b \in R$.

Thus for R_1 we should show that the additive composition is both associative and commutative, Identity and inverse exist and closure property All these would establish that $(R,+)$ is an abelian group and it is called the additive group of the ring.

R_2 **Multiplication composition is associative,**

i e., $(a.b).c=a.(b.c) \ \forall \ a, b, c \in R$

It may be noted that for ring there is no necessity for the existence of multiplicative identity and inverse and also multiplicative composition to be commutative

R_3 **Multiplication is both right and left distributive with regard to addition.**

t.e. $a.(b+c)=a.b+a.c$ Right Distributive Law

and $(b+c).a=b.a+c.a$ Left Distributive Law

The two compositions in the ring are interrelated to each other by the axiom R_3.

Note. Since $+$and. are both binary operations in R it follows that R is closed with respect to both addition and multiplication.

t.e. $\forall \ a, b \in R. \ \ a+b$ and $a.b$ both $\in R$.

Exercise 1

1. (a) *Prove that the set I of all integers with ordinary addition and multiplication as the compositions forms a ring. i.e., $(I, +, .)$ is a ring.*

R_1 **The set I is an abelian group for additive composition.**

(1) Sum of two integers is again an integer. **Closure.**

(2) We know that addition is **associative** in I

i.e., $(a+b)+c=a+(b+c) \ \forall \ a, b, c \in I$

(3) The integer 0 is the **additive identity.**

$\because \ \ a+0=0+a=a \ \forall \ a \in I$

(4) For each integer a there exists an integer $-a$ such that $(-a+a)=0=a+(-a)$. Hence inverse exists.

(5) $a+b=b+a.\ \forall\ a, b \in I.$ **Commutative.**

R_2 **Multiplication is a binary composition and is associative.**

$$(ab)\,c=a\,(bc)\ \forall\ a, b, c \in I.$$

Because multiplication is an associative composition in I.

R_3 **Multiplication distributes addition**

i.e. $a.(b+c)=a.b+a.c$ **(R. D. L.)**

$(b+c).a=b.a+c.a\ \forall\ a, b, c \in I$ **(L. D. L.)**

Hence the system $(I, +, .)$ forms a ring.

Exactly in a similar manner we can prove that the following sets of numbers are rings for addition and multiplication as the two compositions.

(b) *The set of even integers with zero.*

(c) *The set of all real numbers.*

(d) *The set of all rational numbers.*

(e) *The set of all complex numbers.*

(f) *The set mI of those integers which are multiples of some given integer m.*

Note. *The set of* **odd integers** *will not constitute a ring for addition and multiplication as the two compositions.*

The sum of two odd integers = even integer

i.e., addition is not a binary operation or closure property is not satisfied. Similarly the set of **natural numbers** is not a ring under the above two compositions as $(N, +)$ will not form a group because inverse of any element in N will not be in N.

2. *Show that the set of numbers given by $a+b\sqrt{2}$ where a and b are integers is a ring with ordinary addition and multiplication as the two compositions.* **(Allahabad 65)**

Let the given set be denoted by $I(\sqrt{2})$ and $a_1+b_1\sqrt{2}$ and $a_2+b_2\sqrt{2}$ be any two elements of this set.

R_1 **The set $[I(\sqrt{2}), +]$ is an abelian group.**

Closure $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})=(a_1+a_2)+(b_1+b_2)\sqrt{2}$
$=A+B\sqrt{2}\in I(\sqrt{2})$

Associative. $\{(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})\}+(a_3+b_3\sqrt{2})$
$=\{(a_1+a_2)+(b_1+b_2)\sqrt{2}\}+(a_3+b_3\sqrt{2})$
$=(a_1+a_2+a_3)+(b_1+b_2+b_3)\sqrt{2}$
$=(a_1+b_1\sqrt{2})+\{(a_2+a_3)+(b_2+b_3)\sqrt{2}\}$
$=(a_1+b_1\sqrt{2})+\{(a_2+b_2\sqrt{2})+(a_3+b_3\sqrt{2})\}$

Identity. $0+0\sqrt{2}\in I(\sqrt{2})$ is the identity.

Inverse. The inverse of any element $a_1+b_1\sqrt{2}$ is $-a_1-b_1\sqrt{2}$ and it belongs to the set $I(\sqrt{2})$

Commutative. $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})$
$=(a_2+b_2\sqrt{2})+(a_1+b_1\sqrt{2})$

$\because$ $(a_1+a_2)+(b_1+b_2)\sqrt{2}=(a_2+a_1)+(b_2+b_1)\sqrt{2}$

$\therefore$ The set $(I\sqrt{2}, +)$ is an abelian group.

R_2 **Multiplication is a binary operation and is associative**

The set $I(\sqrt{2})$ is closed w.r.t. multiplication composition

or $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}$
$=\alpha+\beta\sqrt{2}\in I(\sqrt{2})$.

Also it is easy to verify that

$\{(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})\}.(a_3+b_3\sqrt{2})$
$=(a_1+b_1\sqrt{2}).\{(a_2+b_2\sqrt{2})(a_3+b_3\sqrt{2})\}$

i.e. $(A.B).C=A.(B.C)$ *i.e.*, Associative.

R_3 **Multiplication distributes addition**

i.e., $A.(B+C)=A.B+A.C$.

or $(a_1+b_1\sqrt{2}).[(a_2+b_2\sqrt{2})+(a_3+b_3\sqrt{2})]$
$=(a_1+b_1\sqrt{2}).[(a_2+a_3)+(b_2+b_3)\sqrt{2}]$
$=\{a_1(a_2+a_3)+2b_1(b_2+b_3)\}+\sqrt{2}\{b_1(a_2+a_3)+a_1(b_2+b_3)\}$
$=(a_1a_2+2b_1b_2)+\sqrt{2}\{b_1a_2+a_1b_2\}+(a_1a_3+2b_1b_2)+\sqrt{2}\{b_1a_3+a_1b_3\}$
$=(a_1+b_1\sqrt{2}).(a_2+b_2\sqrt{2})+(a_1+b_1\sqrt{2}).(a_3+b_3\sqrt{2})$

Similarly we can show that

$$(B+C).A=B.A+C.A$$

Thus both right and left distributive laws are satisfied.

Hence the set $[I(\sqrt{2}), +, .]$ is a ring.

Ring of Matrices.

3. *Prove that the set M_n of all $n\times n$ martices is a ring w.r.t. addition and multiplication of matrices. The elements of matrices are numbers belonging to any of the rings of numbers of Ex. 1.* **(Kanpur 69; Lucknow 69; Delhi 70; Meerut B. Sc. Summer 69; Allahabad 67)**

R_1 The set $(M_n, +)$ is an abelian group.

Closure. The sum of two $n\times n$ matrices is again a matrix of $n\times n$ type.

Associative. $(A+B)+C=A+(B+C)\ \forall\ A, B, C \in M_n$ because addition of matrices is associative

Identity. $O_{n\times n}$ *i.e.* the null matrix is the identity.

Commutative $A+B=B+A\ \forall\ A, B \in M_n$.

because matrix addition is commutative.

$\therefore$ The set $(M_n, +)$ is an abelian group.

R_2 Multiplication is a binary operation which is associative.

We know that the product of $n\times n$ matrices is again a $n\times n$ matrix and hence closure property for multiplication is satisfied.

Also we know that $(A.B).C=A.(B.C)\ \forall\ A, B, C \in M_n$. We know that matrix multiplication is associative provided the given matrices are conformable for matrix multiplication and hence in this case since all the matrices are $n\times n$ type they are comformable for matrix multiplication.

R_3 Multiplication distributes addition.

It is true because matrix multiplication distributes

addition *i.e.* $A.(B+C)=A.B+A.C$
$(B+C).A=B.A+C.A$ $\forall\ A, B, C \in M_n$

Hence the set $(M, +, .)$ is a ring.

Ring of residue classes modulo m

4. *Prove that the set of residue classes modulo the +ive integer m is a ring with respect to addition and multiplication of residue classes (mod m)* **(Allahabad 66, 70)**

Let the set $R=[\{0\}, \{1\}, \{2\},\ldots\ldots, \{m-1\}]$
and $\{r_1\}$ and $\{r_2\}$ be any two elements of R,

R_1 The set $(R, +)$ is an abelian group.

We have proved in Theorem 3 P. 43 that $(R, +)$ is an abelian group.

The entire procedure should be reproduced here.

R_2 Multiplication is a binary operation which is associative

This we have proved in therem 5 P. 44

R_3 Multiplication distributes addition.

$$\{r_1\}[\{r_2\}+\{r_3\}]=\{r_1\}.\{r_2+r_3\}$$
$$=\{r_1r_2+r_1r_3\}$$
$$=\{r_1r_2\}+\{r_1r_3\}$$
$$=\{r_1\}\{r_2\}+\{r_1\}.\{r_3\}.$$

If r_1r_2 and r_1r_3 are greater then m and then they are reduced mod m.

Similarly we can prove left distributive law.

Hence the set $(R, +, .)$ is a ring,

5 *Prove that the set {0, 1, 2, 3, 4} is a ring w.r.t addition and multiplication modulo 5.*

Let the given set be denoted by R,

R_1 The set $(R, +_5)$ is an abelian group

We have proved this in Ex. 25. P. 33.

R_2 . Multiplication modulo 5 is a binary operation which is associative.

Preparing a composition table for multiplication modulo 5 we can easily establish that the set is closed under the operation of multiplication modulo 5.

Also $(a \underset{5}{\times} b) \underset{5}{\times} c = a \underset{5}{\times} (b \underset{6}{\times} c) \ \forall\ a, b, c \in R$

As a, b, c are numbers they obey the associative law.

R_3 Multiplication distributes addition

$$a \underset{5}{\times} (b \underset{6}{+} c) = a \underset{5}{\times} b \underset{5}{+} a \underset{5}{\times} c$$

and $$(b \underset{5}{+} c) \underset{5}{\times} a = b \underset{5}{\times} a \underset{5}{+} c \underset{5}{\times} a \quad \forall\ a, b, c \in R.$$

you may show it by actually computing the result from the composition tables by taking a, b, c to be any three elements of the set.

Hence the set $(R, +_5, \times_5)$ is a ring.

Similarly we can show that the set

$(R, +_6, \times_6)$ is a ring where $R = \{0, 1, 2, 3, 4, 5\}$

Ring of functions.

6. *Show that the set R of all real valued continuous functions of x defined over the interval [0, 1] form a ring w.r.t. addition and multiplication defined as follows*

$$(f+g)\ x = f(x) + g(x)$$
$$(f.g)\ x = f(x).g(x) \qquad \textbf{(Raj. M. Sc. 66)}$$

R_1 The set (R, +) is an abelian group

1. Closure. The sum of two continuous functions is again a continuous function.

2. Associative. $[(f+g)+h]\ x = (f+g)\ x + h(x)$ by def.
$= [f(x) + g(x)] + h(x).$

But $f(x)$, $g(x)$, $h(x)$ are real numbers and addition of real numbers is associative and hence

$$= f(x) + [g(x) + h(x)]$$
$$= f(x) + [(g+h)\ x]$$
$$= [f + (g+h)]\ x.$$

$\therefore \quad (f+g)+h=f+(g+h).$ $\qquad \forall\ f, g, h \in R,$

Hence associative

3. Identity. The function O defined as $O(x)=0$ is the identity of the set R.

$\because \quad (O+f)\ x=O\ (x)+f\ (x)=o+f\ (x)=f\ (x).$

$\therefore \quad O+f=f.$

Similarly $f+O=f.$

4. Inverse. The function $-f$ such that $(-f)\ x=-[f\ (x)]$ is the additive inverse of f

$\because\ [(-f)+f] = (-f)\ (x)+f\ (x)=-f\ (x)+f\ (x).$

$=0=O\ (x)$

$\therefore \quad (-f)+f=O$ the identity.

5. Commutative. $(f+g)\ x=f\ (x)+g\ (x)=g\ (x)+f\ (x)$

$=(g+f)\ x$ as addition of real numbers is commutative.

$\therefore \quad f+g=g+f$

R_2 Multiplication is a binary operation which is associative.

The product of two continuous functions is again a continuous function and hence closed for multiplication.

Now $[(f.g).h]\ x=[f\ .\ g]\ (x)\ h\ (x)$ by def.

$=[f\ (x)\ g\ (x)]\ h\ (x).$

But $f\ (x)$, $g\ (x)$ and $h\ (x)$ are real numbers and they are associative

$=f\ (x).[g\ (x).h\ (x)]$

$=f\ (x)\ [(gh)\ x]$

$=[f\ (gh)]\ x$

$\therefore \quad (fg)\ h=f\ (gh)\ \forall\ f, g, h, \in R.$

R_3 Multiplication distributes addition

$[f\ (g+h)]\ x=f\ (x).\ (g+h)\ (x)$ by def.

$=f\ (x).[g\ (x)+h\ (x)]$

$=f\ (x).g\ (x)+f(x).h\ (x)$

$$=(fg)\,x+(fh)\,x$$
$$=(fg+fh)\,x.$$

$\therefore\ f(g+h)=fg+fh \qquad \forall\ f, g, h \in R$

Similarly $(g+h)\,f=gf+hf.$

Hence the set $(R, +, .)$ **is a ring**

Null or zero ring

7. *The singleton,* $\{0\}$ *is a ring w.r.t. addition and multiplication.*

$0+0=0$ and $0.0=0.$

The above ring is celled null ring.

§ 2. General properties of rings

If R be a ring with respect to addition and multiplication and $a, b, c \in R$ *then prove the following.*

(A) $a.0=0.a=0.$ **(Lucknow 69; B. H. U. 68; Meerut B. Sc. 68, 70, M. Sc. 70)**

Proof. $0=0+0$

$a.0=a.(0+0)=a.0+a.0.$ (R. D. L.)

$\therefore\ -(a.0)+a.0=-(a.0)+a.0+a.0$

$0=\{-(a.0)+a.0\}+a.0.$ Associative

$0=0+a.0=a.0$

Similarly $0.a=(0+0).a=0.a+0.a$ L. D. L.

we can show that $0.a=0.$

(B) $-a.(-b)=-(a.b)=(-a).b.$

(Bombay 70; Meerut B. Sc. 68; M. Sc. 67; Allahabad 64)

We know that $a.0=0$

or $a\,[(-b)+b]=0 \Rightarrow a(-b)+a\,b=0$ R. D. L.

$[a\,(-b)+a.b]+\{-(a.b)\}=0+\{-(ab)\}$

$\Rightarrow a\,(-b)+[a\,b+\{-(a.b)\}]=-(a.b)$ Associative

$\Rightarrow a\,(-b)+0=-(a.b) \Rightarrow a\,(-b)=-(a.b)$

Similarly $0.b=0 \Rightarrow (-a+a).b=0$

$\Rightarrow (\ a).b+a.b=0$

$\Rightarrow [(-a).b+a.b]+\{-(a.b)\}=0+\{-(a.b)\}$

$\Rightarrow \quad (-a).b+[a.b+\{-(a.b)\}]=-(a.b)$

$\Rightarrow \quad (-a).b+0=-(a.b)$

$\Rightarrow \quad (-a).b=-(a\,b).$

(C) $(-a).(-b)=a.b.$ **(Meerut 67, 68)**

We know that $a.(-b)=-(a\,b)$ by B

writing $-a$ for a in the above.

$$(-a).(-b)=-[(-a).b]=-[-(a.b)]=a.b.$$

Because we know that inverse of an inverse of an element is the element itself *i.e.*, $(a^{-1})^{-1}=a$ for multiplicative composition

and $-(-a)=a$ for additive composition.

(D) $a.(b-c)=a.b-a.c,\ (b-c).a=b.a-c.a$

(Benaras 68; Meerut B. Sc. 70; Allahabad 64)

$a.\ (b-c)=a\,[b+(-c)]=a.b+a.(-c)$ R. D. L.

$=a.b+[-(a.c)]$ by B.

$=a.b-a.c.$

$(b-c).a=[b+(-c)]\,a=b.a+(-c).a$ L.D.L

$=b\,a+[-(c.a)]$ by B

$=b.a-c.a$

Note. *From D we conclude that both right and left distributive laws hold good for subtraction also.*

§ 3. Types of rings.

1. Commutative rings. (Kanpur B. Sc. stat 68)

The ring $(R, +,.)$ is said to be a commutative ring if its multiplication composition is also commutative.

i.e. $ab=ba\ \forall\ a, b \in R.$

Refering to Ex. 1–6 on P. 169–176 we say that all the rings of numbers of example (1) are commutative rings as the multiplication of numbers is commutative. Similarly the rings of Ex. 2, 4, 6 are also commutative. But the ring of matrices of Ex. 3 is not commutative because matrix multiplication is not commutative in general *i.e.* AB is not equal to BA in general.

2. Rings with unity, **(Kanpur M. Sc. stat 68)**

The ring $(R, +, .)$ is said to be a ring with unity if it contains an element denoted by 1 such that $a.1=1.a=a \ \forall \ a \in R$.

The unit element 1 is called **multiplicative identity.** It should not be confused with integer 1 though both are denoted by the same symbol.

In the ring of integers the element 1 is the integer 1 whereas in the ring of matrices the unit element is the unit matrix of suitable order. In the ring of all even integers there is no unit element and as such it is a ring without unity. Similarly in Ex. 6 P. 174 the function e defined by $e(x)=1 \ \forall \ x \in [0, 1]$ is the unit element because in this case $(ef)\ x=e(x).f(x)=1.f(x)=f(x).1=f(x). \ \therefore \ ef=f.$

Similarly $(fe)\ x=f(x).e(x)=f(x).1=f(x).$

$$\therefore \quad fe=f$$

Ex. *Give an example of each of the following.*

(a) a commutative ring without unitv.

(b) a non commutative ring with unity. **(Delhi 1970)**

(a) Ring of even integers is certainly a commutative ring but it is without unit element. **See Ex. I (a, b) P. 170**

(b) Ring of $n \times n$ matrices is certainly a ring with unity, the unit element being the unit matrix of suitable order but it is not commutative ring. **Ex. 3 P. 172**

3. Inversible elements in a ring with unity.

If a ring $(R, +, .)$ be a ring with unity then an element $a \in R$ is called inversible if there exists an element $b \in R$ such that $a.b=1=b.a$. In this case we write $b=a^{-1}$.

In a ring of all integers which is a ring with unity the only inversible elements are $1, -1$. The element 2 is not inversible because $1.\frac{1}{2}=1=\frac{1}{2}.2$ but $\frac{1}{2}$ does not belong to the set of all integers.

Similarly in a ring of all $n \times n$ matrices with **real numbers** as elements whose unit element is the unit matrix, all the matrices are not inversible. Only those matrices which are non-singular *i.e.*, whose determinants are not zero are inversible as in that case $AB=BA=I$ then $B=A^{-1}$.

4. Rings with zero divisors.

A ring $(R, +.)$ *is said to be a ring with zero divisors if for* $a, b \in R$ *we have* $ab=0$ *though* $a \neq 0$, $b \neq 0$,
i.e., product of two non-zero elements of R is zero without any of them being zero.

In this case a and b are said to be proper divisors of zero.

Such divisors can not arise in the rings of numbers for as we know the product of two non-zero numbers can never be zero without either or both of them being zero.

But in the ring of matrices we can have the product of two non- zero matrices as a zero matrix.

For example $\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$

$$\begin{bmatrix}0 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}2 & 7\\0 & 0\end{bmatrix}=\begin{bmatrix} & 0\\0 & 0\end{bmatrix}$$

i.e. $AB=O$ (null or zero matrix)

Here neither A nor B is a zero matrix but their product is a zero matrix. Hence A and B are divisors of zero and the ring is said to be a ring with zero divisors.

Similarly we have shown that the set

$R=\{0, 1, 2, 3, 4, 5\}$ is a ring.
$\quad\quad\quad

5. Ring without zero divisors.

A ring $(R, +, .)$ is said to be a ring without zero divisors if the product of no two non-zero elements of the same is zero i.e. $ab=0 \Rightarrow a=0$ *or* $b=0$ *or* $a=0$ *and* $b=0$.

Read the following example no I carefully for the sake of clarification. **Exercise 2**

Ex. 1 *The set* $R=\{a, b, c, d\}$ *with addition and multiplication operation defined by the given tables is a ring. Find its zero and unity and classify it.*

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$.$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	c	a
d	a	d	a	d

How to read the table. $c+d$=element at the intersection of row headed by c and column headed by d and it is b *i.e.*, $c+d=b$, similarly $d+b=c$, $a+c=c$ etc.

Similarly from the second table $d.c$=element at the intersection of row headed by d and column headed by c and it is a *i.e.*, $d.c=a$ and in a similar manner $c.d=a$, $d.b=d$ and so on.

To prove that the given set is a ring.

R_1 The set (R, +) is an abelian group.

(1) Closure. From the table it is clear that sum of any two elements is again an element of the set.

2 Associative. $(a+b)+c=b+c=d \quad \therefore \quad a+b=b$

$a+(b+c)=a+d=d. \quad \because \quad b+c=d$

$\therefore \quad (a+b)+c=a+(b+c).$

3 Identity. $a+a=a$, $a+b=b=b+a$,

$a+c=c=c+a$, $a+d=d=d+a$.

Hence the element a is the additive identity of the set and it is called zero of the ring.

(4) **Inverse.** From the table it is clear that

$$a+a=a,\quad b+b=a,\quad c+c=a,\quad d+d=a,$$

where a is identity, Hence each element is its own inverse.

(5) **Commutative.** Since $c+d=b$ and $d+c=b$

i.e., $c+d=d+c$ Similarly we can verify that $\forall\ x,y \in R\ x+y=y+x$ and hence commutative.

R_2 Multiplication is a binary operation which is associative.

From the second composition table it is clear that product of any two elements is again an element of the set.

Also $(b.c).d=c.d=a.\ \because\ b\ c=c$

$b.(c.d)=b.a=a.\ \because\ c.d=a$

$\therefore\quad (b.c).d=b.(c\ d)$ and hence associative

R_3 Multiplication distributes addition.

$$b.(c+d)=b.b=b.$$

$$b.c+b.d=c+d=b$$

$$\therefore\quad b.(c+d)=b.c+b.d$$

Similarly $(c+d).b=c.b+d.b$

Hence the given set is a ring under given compositions.

The ring is commutative.

From the table it is clear that

$c.d=d.c=a;\ a.b=b.a=a;\quad b.c=c.b=c$ etc.

Unity of the ring [*i.e.*, multiplicative identity.].

From the table it is clear that b is multiplicative identity *i.e.*, unity of the ring

$\because\ a\ .\ b=b\ .\ a=a;\ b\ .\ b=b,\ c\ .\ b=b\ .\ c=c,\ d\ .\ b=b\ .\ d=d$

i.e. $x\ .\ b=b\ .\ x=x\ \forall x \in$ Ring.

Zero of the ring [*i.e.*, additive identity]

From the first table $a+a=a;\ b+a=a+b=b;$

$$c+a=a+c=c;\ d+a=a+d=d$$

and hence a is the additive identity or zero of the ring.

$\because \quad a+x=x+a=x \ \forall \ x \in$ Ring.

The ring is with zero divisors.

We have from the table $c \,.\, d=a$, *i.e.*, zero of the ring *i.e.*, product of two non zero elements is zero and hence it is a ring with zero divisors, c and d being the divisors of zero.

Inversible elements of the ring.

The element a is inversible if there exists an element b such that $a \,.\, b=$unity of the ring.

Here b is the unity of the ring and from the table we observe that only $b \,.\, b=b=$unity, so b is the only inversible element and its inverse being itself. Product of no other two elements is equal to unity *i.e.*, b of the ring,

Do the above question taking the composition tables as under.

(*a*)

+	*a*	*b*
a	*a*	*b*
b	*b*	*a*

.	*a*	*b*
a	*a*	*a*
b	*a*	*b*

+	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*a*	*d*	*c*
c	*c*	*d*	*a*	*b*
d	*d*	*c*	*b*	*a*

.	*a*	*b*	*c*	*d*
a	*a*	*a*	*a*	*a*
b	*a*	*b*	*c*	*d*
c	*a*	*c*	*d*	*b*
d	*a*	*d*	*b*	*c*

Ans. Yes *a* ring, *a* is zero and *b* the unity of the ring. *b*, *c*, *d* are inversible elements, *a* is not inversible because $b \cdot b=b$, $c \cdot d=b$, $d \cdot c=b$.

The unity element *b* is not present is the first row and as such *a* is not inversible. It is commutative.

It is a ring without zero divisors because the product of no two non-zero element *b*, *c* or *d* is zero *i.e.*, *a*

(b)

+	*a*	*b*	*c*	*d*
a	*a*	*b*	*c*	*d*
b	*b*	*a*	*d*	*c*
c	*c*	*d*	*a*	*b*
d	*d*	*c*	*b*	*a*

·	*a*	*b*	*c*	*d*
a	*a*	*a*	*a*	*a*
b	*a*	*b*	*c*	*d*
c	*a*	*a*	*a*	*a*
d	*a*	*b*	*c*	*d*

Yes, *a* ring, *a* is zero. It is a ring without unity. It is not commutative because $c \cdot d=a$ and $d \cdot c=c$.

2. (a) *Find the multiplicative inverse of the element* $\begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}$ *of the ring of all matrices of order two over the integers.*

Let any 2×2 matrix $\begin{bmatrix} x & y \\ z & u \end{bmatrix}$ be the inverse of given matrix where x, y, z, u all belong to I. The unity of the ring is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

$$\therefore \quad \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} x & y \\ z & u \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

or
$$\begin{bmatrix} 2x+5z & 2y+5u \\ x+3z & y+3u \end{bmatrix}=\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$\therefore \quad 2x+5z=1,\ x+3z=0,\ 2y+5u=0,\ y+3u=1.$

Solving we get $x=3,\ y=-5,\ z=-1,\ u=2.$

Therefore $\begin{bmatrix}2 & 5\\ 1 & 3\end{bmatrix}^{-1}=\begin{bmatrix}3 & -5\\ -1 & 2\end{bmatrix}$.

(b) *Show that the set M of all matrices of order two over the integers of the form* $\begin{bmatrix} x & y\\ z & u\end{bmatrix}$ *forms a ring* $(M, +, .)$, *Verify the associative law of multiplication and the distributive law. What is zero of the ring. Verify that* $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ *is the unity of the ring.* **(Allahabad 67; Delhi 70; Meerut B. Sc. Summer 69)**

Proceed exactly as in Ex. 3 P. 172 for proving a ring.

Verification. Let $A=\begin{bmatrix}1 & 1\\ -1 & 0\end{bmatrix},\ B=\begin{bmatrix}2 & 0\\ 3 & 1\end{bmatrix},$

$$C=\begin{bmatrix}-1 & 2\\ 1 & 4\end{bmatrix}$$

you may choose A, B, C in any manner. Now you should show by actual tabulation that

$$(AB)\,C=A\,(BC).$$

and $$A\,(B+C)=AB+AC$$

$$(B+C)\,A=BA+CA.$$

Also $$AB=\begin{bmatrix}1 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}2 & 0\\ 3 & 1\end{bmatrix}=\begin{bmatrix}5 & 1\\ -2 & 0\end{bmatrix}$$

$$BA=\begin{bmatrix}2 & 0\\ 3 & 1\end{bmatrix}\begin{bmatrix}1 & 1\\ -1 & 0\end{bmatrix}=\begin{bmatrix}2 & 2\\ 2 & 3\end{bmatrix}$$

Clearly $AB\neq BA$. So that the ring is not a commutative ring. The zero of the ring is $\begin{bmatrix}0 & 0\\ 0 & 0\end{bmatrix}$ and its unity is $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$.

Also it is a ring with zero divisors because

$$\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\begin{bmatrix}0 & 0\\1 & 0\end{bmatrix}=\begin{bmatrix}0 & 0\\0 & 0\end{bmatrix}$$

i.e., $AB=O$ when neither A nor B is null matrix *i.e.*, zero.

3. *Classify the ring whose elements are* $a+b\sqrt{2}$ *where a and b are integers.*

We have already proved that the set

$$\{a+b\sqrt{2} \ : \ a, b \in I\}_{+.}$$

is a ring. (P. 170)

Since $(a_1+b_1\sqrt{2})\ (a_2+b_2\sqrt{2})=(a_2+b_2\sqrt{2})\ (a_1+b_1\sqrt{2})$ it is a **commutative ring.**

It is also **ring with unity,** the unit element being $1+0\sqrt{2}$, which belongs to the set.

$$AB=(a_1+b_1\sqrt{2})\ (a_2+b_2\sqrt{2})$$
$$=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\ \sqrt{2}.$$

Now $AB=0$ if both $a_1a_2+2b_1b_2=0$

$$a_1b_2+b_1a_2=0,$$

These two will hold only if either $a_1=0, b_1=0$ or $a_2=0, b_2=0$ and for no other set of values both will be zero.

Hence if $a_1=0, b_1=0$ then $a_1+b_1\sqrt{2}$ *i.e.*, $A=0$.

$\therefore$ $AB=0$ if $A=0$ or if $B=0$,

Hence it is a **ring without zero divisors.**

4. *Classify the ring formed by a set of even integers with addition and multiplication as the two compositions.*

Proceding as in **Ex. 1 P. 169** we can show that the set $(2I, +.)$ forms a ring. It is **commutative.** It is a ring **without unity** because in the ring of numbers the unit element is 1 and does not belong to the set $2I$. It is also a ring without zero divisors because the product of two non-zero even numbers can never be zero.

5. *Show that the set of residue classes modulo p a +ive integer is a ring w. r. t. addition and multiplication*

modulo p. Also show that if p is prime the ring has no zero divisors but if p is composite then the ring is with zero divisors. **(Bombay 70; Allahabad 70. 66; Raj. Sc. 66)**

We have already proved in **Ex. 4 P. 173** the first part.

{0} is the identity of the additive group *i.e.*, zero of the ring.

Ist Case. p is prime.

Let $\{r\}$ and $\{s\}$ be any two elements of the ring.

then $$\{r\}.\{s\}=\{0\} \Rightarrow \{rs\}=\{0\}$$
$$\Rightarrow rs=0 \bmod p.$$

Since p is prime rs can never be equal to 0 (mod p) unless one of them say r is p itself *i.e.*, $r=0 \bmod p$ or $\{r\}=\{0\}$.

Here $\{r\}.\{s\}=0$ only if $\{r\}=0$ *i.e.*, zero or $\{s\}=\{0\}$.

Therefore in this case it is a **ring without zero divisors**—Also it is commutative with unity element {1}.

2nd Case. p is composite.

Let $p=rs$, so that $rs=0 \pmod p$ $\therefore$ $\{rs\}=\{0\} \pmod p$.

Now $\{r\}.\{s\}=\{rs\}=\{0\}$ *i.e.*, zero of the ring.

Here neither $\{r\}$ nor $\{s\}$ are zero *i.e.*, {0} mod. p, but their product is {0}.

Hence in this case it is a ring **with zero divisors.** Also it is commutative.

6. *Prove that the set R of ordered pairs (a, b) of real numbers is a ring with zero divisors, which is commutative and is a ring with unity under the addition and multiplication defined as.*

$$(a, b)+(c, d)=(a+c, b+d)$$
$$(a, b).(c, d)=(ac, bd) \quad \forall\ (a, b), (c, d) \in R.$$

R_1 The set (R, +) is an abelian group.

Closure . $(a, b)+(c, d)=(a+c, b+d) \in R.$

Associative : $[(a, b)+(c, d)]+(e, f)$
$=(a+c, b+d)+(e, f)$
$=[(a+c)+e, (b+d)+f]$
$=[a+(c+e), b+(d+f)]$
As addition of numbers is associative.
$=(a, b)+[(c+e), (d+f)]$
$=(a, b)+[(c, d)+(e, f)]$.

Identity : The ordered pair $(0, 0)$ is the identity.
$\because$ $(a, b)+(0, 0)=(a+0, b+0)=(a, b)$.

Inverse : The inverse of any ordered pair
(a, b) is $(-a, -b) \in R$.
$\because$ $(a, b)+(-a, -b)=(a-a, b-b)=(0, 0)$ *i.e.*, identity

Commutative : $(a, b)+(c, d)=(a+c, b+d)=(c+a, d+b)$
$=(c, d)+(a, b)$.

This is so because addition of real numbers is commutative.

R_2 Multiplication is a binary operation which is associative.

$(a, b).(c, d)=(ac, bd) \in R$ and hence closed for multiplication.

Also $[(a, b).(c, d)].(e, f)=(ac, bd).(e, f)$
$=[(ac)\ e, (bd)\ f]=[a\ (ce), b\ (df)$
$=(a, b).(ce, df)=(a, b)\ [(c, d).(e, f)]$.

This is so as multiplication of real numbers is associative

R_3 Multiplication distributes addition.

$(a, b)\ [(c, d)+(e, f)]=(a, b)\ [c+e, d+f]$
$=[a\ (c+e), b\ (d+f)]=[ac+ae, bd+bf]$
by distributive law of real numbers
$=(ac, bd)+(ae, bf)=(a, b)\ (c, d)+(a, b)\ (e, f)$.

Similarly we can prove left distributive law.

Hence R is ring whose zero element is (0, 0).

It is also a commutative ring.

$$(a, b) \cdot (c, d)=(ac, bd)=(ca, db)=(c, d) \cdot (a\ b)$$

it is a ring with unity.

$$(a, b) \cdot (1, 1)=(a.1, b.1)=(a, b)\ \forall\ (a, b) \in R.$$

The unit element being (1, 1)

It is a ring with zero divisors.

In order to show that it is a ring with zero divisors we have to show that there exist two non-zero ordered pairs whose product is zero of ring.

e.g. $(a, 0) \cdot (0, d)=(a \cdot 0, 0 \cdot d)=(0, 0)$.

Neither of the ordered pair on the left is zero, but their product is zero and as such it is a ring with zero divisors.

7. *If two operations * and o on the Z of integers are defined as under*

$$a * b=a+b-1 \qquad a\ o\ b=a+b-ab$$

*Prove that system (Z, *, o) is a commutative ring with unity.*

(Benares 70)

R_1 Refer Ex. 15 P. 20 we have already shown that the set Z is an abelian group for the composition * defined as given.

R_2 **The composition o is binary and associative.**

Clearly $a\ o\ b=a+b-a\ b \in Z$ and hence binary.

Again $(a\ o\ b)\ oc=(a+b-ab)\ oc$

$$=a+b-ab+c-(a+b-ab)\ c$$
$$=a+b-ab+c-ac-bc+abc$$

Again $ao\ (b\ o\ c)=ao\ (b+c-bc)$

$$=a+b+c-bc-a\ (b+c-bc)$$
$$=a+b+c-bc-ab-ac+abc$$

$\therefore$ $(a\ o\ b)\ o\ c=ao\ (b\ o\ c)$ Hence associative.

R_3 o is distributive over *

$$ao\ (b * c)=ao\ (b+c-1)$$

$$=a+b+c-1-a(b+c-1)$$
$$=a+b+c-1-ab-ac+a$$
$$=2a+b+c-1-ab-ac$$

Again $a \circ b=a+b-ab$

$a \circ c=a+c-ac$

$\therefore \quad (a \circ b) * (a \circ c)=(a+b-ab) * (a+c-ac)$
$=a+b-ab+a+c-ac-1$
$=2a+b+c-1-ab-ac$

$\therefore \quad a \circ (b * c)=(a \circ b) * (a \circ c)$ Hence right distributive law.

Similarly we can prove the left distributive law.

Commutative. Since $a\,b=b\,a \ \forall \ a, b \in Z$

$\therefore \quad a \circ b=a+b-a\,b=b+a-ba=b \circ a$

Unity. $a \circ 0=a+0-a.0=a$

$0 \circ a=0+a-0.a=a$

$\therefore \quad a \circ 0=a=0.a$

Hence 0 is the unity of the ring thus the given set is a commutative ring with unity for the two compositions defined as given.

8. *Prove that the set*

$$A=\{a+b\,3^{1/3}+c.3^{2/3} : a, b, c \in Q\}$$

is a ring with respect to addition and multiplication.

(B. H. U. 70)

9. *If R is a system satisfying all the conditions for a ring with unit element* **with the possible exception** *of*

$$a+b=b+a \ \forall \ a, b \in R,$$

Prove that the axiom $a+b=b+a$ must hold in R and that R is thus a ring. **(Delhi 70)**

Method. Here we shall make use of all the postultates of a ring *i.e.* $(R, +)$ is a group (though not abelian because

of the exception of $a+b=b+a$). Both right and left distributive laws, multiplication is associative. Also in a ring with unity the element $1 \in R$. By making use of the above postulates we shall establish $a+b=b+a$ must hold good so that the exception given is ruled out and it becomes a ring.

Now 1 is the unit element of the ring such that

$$a.1=1.a=a$$

$$(a+b)\,(1+1)=a\,(1+1)+b\,(1+1) \text{ by L. D. Law}$$

$$=(a.1+a.1)+(b.1+b.1)$$

by R. D. Law

$$=(a+a)+(b+b). \qquad \ldots(1)$$

$\because$ 1 is the unit element.

Again $(a+b)\,(1+1)=(a+b).1+(a+b).1$ by R. D. Law

$$=(a.1+b.1)+(a.1+b.1)$$

by L. D. Law

$$=(a+b)+(a+b) \qquad \ldots(2)$$

$\because$ 1 is unit element.

$\therefore$ $(a+a)+(b+b)=(a+b)+(a+b)$ by (1) and (2)

or $[(a+a)+b]+b=[(a+b)+a]+b.$

$\because$ $+$ is associative.

or $(a+a)+b=(a+b)+a$ by R. Can. Law.

or $a+(a+b)=a+(b+a)$ $\because$ $+$ is associative.

or $a+b=b+a$ by L. Can. Law.

Above rules out the given exception of addition being commutative. Hence the given system must form a ring.

10. *If R is a ring such that $a^2=a \;\forall\; a \in R$, prove the following*

(*i*) $a+a=0 \;\forall\; a \in R$. *i.e. each element is its own additive inverse.*

(2) $a+b=0 \Rightarrow a=b$.

(3) *R is a commutative ring i.e.* $a.b=b.a \ \forall \ a, b \in R$.
(B. H. U. 70; Kurkhetra 69; Kanpur 70; Delhi 69; Punjab 66)

Proof. (1) $a \in R \Rightarrow a+a \in R$.

$\therefore \quad (a+a)^2=a+a$ by given condition

$\Rightarrow (a+a)\ (a+a)=a+a$

$\Rightarrow (a+a)\ a+(a+a)\ a=a+a$ by R. D. Law

$\Rightarrow (a^2+a^2)+(a^2+a^2)=a+a$ by L. D. Law

$\Rightarrow (a+a)+(a+a)=(a+a) \quad \because \quad a^2=a$

$\Rightarrow (a+a)+(a+a)=(a+a)+0$

$\because \quad x+0=x \ \forall \ x \subset R$

$\Rightarrow a+a=0$ by L. C. Law.

(2) $a+b=0 \Rightarrow a+b=a+a \quad \because \quad a+a=0 \ \forall \ a \in R$ by (1)

$\Rightarrow b=a$ by L. C. Law.

(3) $a \in R, b \in R \Rightarrow a+b \in R$

$\Rightarrow (a+b)^2=a+b$ by given condition.

$\Rightarrow (a+b)\ (a+b)=a+b$

$\Rightarrow (a+b)\ a+(a+b)\ b=a+b$ by R. D. Law

$\Rightarrow a^2+ba+ab+b^2=a+b$ by L. D. Law

$\Rightarrow (a+ba)+(ab+b)=a+b \quad \because \quad a^2=a, \ b^2=b$

$\Rightarrow (a+b)+(ba+ab)=(a+b)+0$

as $+$ is associative and commutative.

$\Rightarrow ba+ab=0$ by L. C. Law

$\Rightarrow ba=ab \quad \because$ by (2) $a+b=0 \Rightarrow b=a$.

Hence R is a commutative ring.

In a ring if $a^2=a \ \forall \ a \in R$ *i.e.* each element of a ring is idempotent then such a ring is celled a **Boolean Ring.**

§ **4. Cancellation Law in a ring.**

$ab=ac \Rightarrow b=c \ [a \neq 0]$ Left C. L.

$ba=ca \Rightarrow b=c \ [a \neq 0]$ Right C. L.

Now if a ring is with zero divisors

i.e. $ab=0,\ a\neq 0,\ b\neq 0$

then $ab-0=a.0,\ [a\neq 0] \Rightarrow b=0$

by cancellation law. But this is a contradiction as the ring is with zero divisors. **Thus it is not possible for us to define the cacellation law in a ring with zero divisors.**

Theorem I. *A ring R is without zero divisors if and only if cancellation law holds in R.* **(Kanpur M. Sc Stat. 71; Benares 66; Lucknow 69 Allahabad 69)**

Ist Case. Ring is without zero divisors

i.e. $ab=0 \Rightarrow a=0$ or $b=0$ or both are zero.

To prove that the $ab=ac\ [a\neq 0] \Rightarrow b=c$.

Now $ab-ac \Rightarrow a(b-c)=0$

But since the ring is without zero divisors then either or both of a and $b-c$ should be zero. Since $a\neq 0$.

$\therefore\ b-c=0 \Rightarrow b=c$,

Hence cancellation law holds.

Converse. Cancellation law holds.

To prove that the ring is without zero divisors.

Let us suppose that the ring is with zero divisors

i.e. $ab=0,\ a\neq 0,\ b\neq 0$.

Now $ab=0\ \ a.0 \Rightarrow b=0$ by cancellation law which is a contradiction.

Hence our assumption that the ring is with zero divisors is wrong and such it is a ring without zero divisors

§ 5. Integral Domain.

Definition. *A ring $(R, +, .)$ with more than one element is called an integral domain if*

(a) It is a commutative ring.

(b) It is a ring with unity.

(c) It is a ring without zero divisors.

Note. The condition (c) by the help of Theorem 1 P. 192 can be read as

(c) The cancellation law holds

i.e., $ab=ac \Rightarrow b=c$ and $ba=ca \Rightarrow b=c$.

In short form an integral domain is a commutative ring with unity and without zero divisors. **(Utkal 70; Kanpur M. Sc. 70; Allahabad 64; Meerut M. Sc. 68, 70; Gorakhpur 69 Raj M. Sc. 66)**

The idea of saying "with more than one element" is to emphasize that it must have at least one non zero element in it.

The word integral domain arises from the fact that an integral domain has a number of properties common with the ring of integers which we know is a commutative ring, with unity and is without zero divisors *i.e.*, product of no two non-zero integers is zero.

Examples of Integral domain

1. The ring $(I, +, .)$ is an integral domain.
2. The ring $(Q, +,)$ is an integral domain.
3. The ring $(C, +, .)$ is an integral domain.
4. The ring $(R, +, .)$ is an integral domain.
5. We have shown in Ex. 3, P. 185 that the set $a+b\sqrt{2}$ where $a, b \in I$ is a ring which is commutative and has a unit element and also it is without zero divisors and hence it is an integral domain.
6. The ring whose elements are even integers is a commutative ring without zero divisors but since it is a ring without unity and as such it is **not an integral domain** see Ex 4, P. 185.
7. The set of natural numbers **does not form an integral domain** because it is not a ring as it will not form an abelian group for additive composition.

8. *Prove that the set of residue classes modulo p, a +ive integer is a ring w.r.t. addition and multiplication when will it be an integral domain.*

We have already proved in Ex. 4 P. 173 the first part.

Also it is a ring with unity which is commutative and as proved in Ex. 5 P. 185 when **p is prime** it is a ring without zero divisors and hence it is **an integral domain.** In case **p is composite** then it is a ring with zero divisors and hence it is **not an itegral domain**

9. *$R=\{0, 1, 2, 3. 4\}$. The set $(R, +_5, \times_5)$ is a ring.*

We have already proved in Ex. 5 P. 173

1 is the unity of the ring and also it is a commutative ring, also we khow that product of no two non-zero elements under multiplication modulo 5 can never be zero so that it is a ring without zero divisors, so that it is an integral domain.

If however we consider the set

$R=\{0, 1, 2, 3, 4, 5\}$, then the set $(R, +_6, \times_6)$ is a ring as shown earlier in the cuse $2\times 3=0\ (_{\times_6})$, $4\times 3=0\ (_{\times_6})$.
i.e. product of two non-zero elements is zero, showing that it is a ring with zero divisors and hence it is not an integral domain.

10. *Prove that the only idempotent elements of an integral domain D are 0 and 1.*

We know that $0.0=0$ and $1.1=1$ and as such both 0 and 1 are idempotent elements of an integral domain. The element 1 must be there as D is an integral domain *i.e.* a commutative ring with unity without zero division *i.e.* cancellation law holds.

Now we have to prove that 0 and 1 are the only idempotent elements *i.e.* any other element $a\neq 0, \neq 1$ cannot be idempotent.

If possible let a be idempotent so that

$$a.a=a \quad \text{but} \quad a.1=1.a=a.$$

$\therefore \quad a.a=a.1 \Rightarrow a.(a-1)=0 \Rightarrow a=0$ or $a-1=0$

or both are zero as D is without zero divisors which is a contradiction as $a\neq 0, \neq 1$.

Hence only elements of an I. D. which are idempotent are 0 and 1.

§ 6. Field.

Definition. *A ring* $(R, +, .)$ *which has at least two elements is called a field if*

(*a*) *It is a commutative ring*

(*b*) *It is a ring with unity*

(*c*) *All non zero elements are inversible w. r. t. multiplication*

i.e, $a\neq 0$ *then* $\exists$ b *in* R *such that* $ab=ba=1$ (*unity of the ring*) *then* $b=a^{-1}$ *i.e., multiplicative inverse of a.*

(Gorakhpur 69; Utkal 70; Kanpur M.Sc. Stat 69; Benares 63; Meerut 69, 70)

Note. The integral domain and field are both commutative rings with unity and their third property is different *i.e.*, for I. D. it is a ring without zero divisors and for a field it is a ring in which all non zero elements are inversible.

Alternative definition. Combining the above properties we can give an alternate definition of a field as below.

A ring $(R, +, .)$ *with at least two elements is called a field if its* **non zero elements** *form an abelian group under multiplication.*

(Allahabad 68)

The condition R_2 for a ring proves closure and associativity for multiplication. The ring is with unity shows the existence of multiplicative identity. The commutative pro-

perty proves the character of an abelian group. All non zero elements having their inverses proves the existence of inverses.

Hence the above alternative definition.

Exercise 3

1. *The set Q of all rational numbers, or the set R of all real numbers or the set C of all complex numbers are fields w.r.t. addition and multiplication because they are rings with unity and are commutative as we have already proved and at the same time all non zero elements are inversible. They are integral domains also because the above rings are without zero divisors.*

But the set I of all integers is a commutative ring with unity but since all the non zero elements are not inversible except 1 and -1 and hence it is not a field. It is an integral domain alright as it will be a ring without zero divisors.

2. *Show that the set of +ive integers with addition and multiplication modulo p, p being prime is a finite field having p elements.* **(B.H.U. 63; Lucknow 69; Utkal 70; Delhi 70)**

$R=\{0, 1, 2, \ldots, r, s, \ldots, p-1\}$ equipped with addition and multiplication modulo p (prime) compositions.

We have already shown earlier that the above set is a commutative ring with unity In order to show that it is a field we have to show that all non zero elements are inversible.

Let $r \in R$, $0<r<p$ then there will certainly exist some element $s \in R$ such that $r.s=1 \pmod p$ so that s is the inverse of r.

If p were composite say $p=r.s$ then $r.s=0 \pmod p$ and in that case the element r is not inversible and hence the condition that p is prime.

e.g. $R=\{0, 1, 2, 3, 4\}_{,+5,\times 5}$.

$1 \cdot 1 \equiv 1 \pmod 5 = \text{unity}$ $\therefore$ Inverse of 1 is 1
$\times_5$

$2 \cdot 3 \equiv 1 \pmod 5$ $\therefore$ Inverse of 2 is 3

$3 \cdot 2 \equiv 1 \pmod 5$ $\therefore$ Inverse of 3 is 2

$4 \cdot 4 \equiv 1 \pmod 5$ $\therefore$ Inverse of 4 is 4

Hence all the non zero elements are inversible. Therefore it is a field.

It is also an integral domain because it will be a ring without zero divisors when p is prime. If p were composite *i.e.*, $p=6=2\times 3$.

$$R=\{0, 1, 2, 3, 4, 5)_{,+6,\times 6}$$

In this case $2\cdot 1=2$, $2.2=4$, $2.3=0$, $2.4=2$, $2.5=4$ under mod 6 *i.e.*, the inverse of element 2 does not exist because there is no element $a \in R$ such that $2.a \equiv 1$, *i.e.*, unity (mod 6).

3. ***Prove that the set of all real numbers of the form*** $a+b\sqrt{2}$ ***where*** **a and b are rationals** ***forms a field under addition and multiplication.*** **(Allahabad 65; Meerut 69 (S); Kanpur 70)**

We have already shown on Pages 170, 185 that the above set forms a commutative ring with unity. For a field we have to show that all non zero elements are inversible.

Let $a+b\sqrt{2}$ be any element of the ring.

Now $(a+b\sqrt{2}) \cdot \dfrac{1}{(a+b\sqrt{2})} = 1 = \text{unity of the ring.}$

Then the inverse of $a+b\sqrt{2}$ is $\dfrac{1}{a+b\sqrt{2}}$ provided it belongs to the set.

$$\text{Now } \frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \sqrt{2}\left(\frac{-b}{a^2-2b^2}\right)$$

Above is of the form $a+\sqrt{2}\beta$ and also $a^2 \neq 2b^2$ for any rationals a and b.

Hence the inverses of all non zero elements exist and belong to the set.

Therefore the given set is a field w.r.t. the given compositions.

In general the set of all numbers of the form $a+b\sqrt{p}$ where a and b are rationals and p is prime, is a field under addition and multiplication.

Note. In case a, b were restricted to be integers then it will not be a field but only an integral domain as it can be shown to be ring without zero divisors.

(Kanpur 70)

4. $R=\{0, 2, 4, 6, 8\}$.

Prove that the above set is a commutative ring under addition and multiplication modulo 10. Verify whether it is an integral domain or a field or both.

We write the following composition tables for addition and multiplication modulo 10.

$6+8=14=4 \pmod{10}$ $\quad$ $6\times 8=48=8 \pmod{10}$

$+_{10}$	0	2	4	6	8
0	0	2	4	6	8
2	2	4	6	8	0
4	4	6	8	0	2
6	6	8	0	2	4
8	8	0	2	4	6

$\times_{10}$	0	2	4	6	8
0	0	0	0	0	0
2	0	4	8	2	6
4	0	8	6	4	2
6	0	2	4	6	8
8	0	6	2	8	4

It is easy to verify that the above system constitutes a ring. 0 is the zero *i.e.*, additive identity. Looking to the Ist and 5th columns or rows of second table we find that they are identical showing thereby $a \times 6 = 6 \times a = a \ \forall \ a \in R$. Hence 6 is the multiplicative identity *i.e.*, the unity of the ring. The multiplication composition is commutative.

Hence it is a commutative ring with unity. Also from the second table we observe that product of no two non-zero numbers is zero and hence it is a ring without zero divisors. Hence the given system is an integral domain.

Again form the second table we find that all non-zero elements are inversible and hence it is a field also.
e.g., In order to find inverse of 8 run your eye along the row headed by 8 and stop at unity *i e.*, identity element 6 then numbers 2 at the head of the column in which 6 is placed is the inverse of 8.

Similarly inverse of 2 is 8, inverse of 4 is 4, inverse of 6 is 6.

5. *Show that the set of gaussian integers form a ring under ordinary addition and multiplication of complex numbers. Verify whether it is an integral domain or a field.*

Gaussian Integers. Complex numbers of the type $a+ib$ **where a and b are integers** are called gaussian integers. $\frac{2}{5}+\frac{4}{3}i$ is not a gaussian integer because $\frac{2}{5}$ and $\frac{4}{3}$ are not integers.

Proceeding as in Ex. 2 P. 170 we can verify all the postulates of the ring. It is a ring with unity the unit element being $1+0i$ *i e.*, 1. Since product of complex numbers is commutative and as such it is commutative ring. For integral domain it has to be a ring without zero divisors

i.e., $ab=0 \Rightarrow a=0$ or $b=0$ or a and b both are zero.

$$(a+ib)(c+id)=(ac-bd)+i(ad+bc)=0$$
$$\Rightarrow \quad ac-bd=0 \text{ and } ad+bc=0$$
$$\Rightarrow \quad \left.\begin{matrix} ac=bd \\ ad=-bc \end{matrix}\right\} -(A). \text{ Suppose } a\neq 0,\ b=0$$

then multiplying relations in A, we get

$$a^2cd=-b^2cd \Rightarrow cd(a^2+b^2)=0$$
$$\Rightarrow \quad cd=0 \text{ as } a^2+b^2\neq 0.$$

Hence either $c=0$ or $d=0$. If $c=0$ then from A *i.e.*, $ad=-bc$ we get $ad=0 \Rightarrow d=0 \quad \because \quad a\neq 0$.

Hence $c=0, d=0 \Rightarrow c+id=0$. Thus product of two is zero only if one of them is zero. Therefore the ring is without zero divisors and as such it is an integral domain.

For a field we have to show that all non zero elements have their inverses in the set of gaussian integers. Let $a+ib$ be any non-zero element.

$$(a+ib).\frac{1}{(a+ib)}=1 \quad \textit{i.e.}, \text{ unity.}$$

Hence $\dfrac{1}{a+ib}$ is the inverse of $a+ib$.

But $\dfrac{1}{a+ib}=\dfrac{a-ib}{a^2+b^2}=\dfrac{a}{a^2+b^2}+i\left(\dfrac{-b}{a^2+b^2}\right)$ which is not a Gaussian integer because $\dfrac{a}{a^2+b^2}$ and $\dfrac{-b}{a^2+b^2}$ are not integers in general. Hence the inverse does not belong to the set. Therefore it is not a field.

Note. $a^2+b^2\neq 0$ as $a^2+b^2=0 \Rightarrow a=0, b=0$ and in that case $a+ib=0$ but $a+ib$ is a non zero element.

6. *Show that the set* $[a, b, c, d]$ *in which addition and multiplication are defined by the following tables is a finite field.*

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

.	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

Refer Ex. 1 (a, b) P. 180–183. We have shown that the above set is a ring under the given compositions. Further that this is a ring with unity. The unity element being b. Also it is a commutative ring. The zero of the ring is the element a. It is also a ring without zero divisors and hence it is an integral domain. Again the non zero elements of the ring are b, c, d whose inverses from the second table are b, d and c respectively so that all the non zero elements are inversible and as such it is a field.

7. *For the ring* $[\{0, 1, 2, 3, 4, 5, 6\}]_{+_7, \times_7}$
find -2, -5, $-(3 \underset{\times_7}{\times} 5)$, $2 \underset{\times_7}{\times} (-6)$.

We have already shown that the given set constitutes a ring which is a field as 7 is prime.

By -2 we mean additive inverse of 2.

Now $2+5=7\equiv 0 \pmod 7$ = additive identity.

Hence inverse of 2 *i.e.*, -2 is 5.

Similarly inverse of 5 *i.e.*, -5 is 2.

Again $(3\times5)=15=1 \pmod 7$
$\times 7$

$\therefore$ $-(3\times5)=-1$ *i.e.* additive inverse of 1.
$\times 7$

Now $1+6=7=0 \pmod 7$ $\therefore$ Inverse of 1 *i.e.*, -1 is 6.

Again $2\times(-6)=-(2\times6)=-12=-5 \pmod 7$.
$?$ $?$

additive inverse of $5=2$. $\because$ $5+2=7=0 \pmod 7$.

8. *Prove that the set R of ordered pairs (a, b) of real numbers is a field under addition and multiplication defined as follows*

$$(a, b)+(c, d)=(a+c, b+d) \quad \text{.. (1)}$$
$$(a, b)\,.\,(c, d)=(ac-bd, bc+ad). \quad \text{...(2)}$$

Field : (1) It is a commutative ring with unity in which every non zero element is inversible.

For Ring :

R_1 : **(R, +) is an abelian group.**

For this please see the proof of R_1 of Ex. 6 P. 186.

R_2 : **Multiplication is a binary operation which is associative.**

By def. (2) $(a, b)\,.\,(c, d)=(ac-bd,\ bc+ad) \in R$ and hence binary.

Now
$$\begin{aligned}
&[(a, b)\,.\,(c,\ d)]\,(e, f)\\
&=(ac-bd,\ bc+ad)\,(e, f)\\
&=\{(ac-bd)\,e-(bc+ad)\,f,\ \{(bc+ad)\,e\\
&\qquad\qquad +(ac-bd)\,f\}\\
&=\{a\,(ce-df)-b\,(de+cf),\\
&\qquad\qquad b\,(ce-df)+c\,(de+cf)\\
&=(a, b)\{(ce-df),\ (de+cf)\}\\
&=(a, b)\,[(c, d)\,.\,(e, f)].\ \text{Hence associative.}
\end{aligned}$$

R_3 : **Multiplication distributes addition.**

$$(a, b)\,[(c, d)+(e, f)]=(a\ ,\ b)\ (c+e,\ d+f)$$
$$=\{a\ (c+e)-b\ (d+f),\ b\ (c+e)+a\ (d+f)\}$$
$$=\{(ac-bd)+(ae-bf),\ (bc+ad)+(be+af)\}$$
$$=((ac-bd,\ bc+ad))+((ae-bf)+(be+af))$$

by (1)

$$=(a,\ b)\quad (c,\ d)+(a,\ b)\ .\ (e, f).$$

Above proves right distributive law and similarly we can prove left distributive law.

Thus $(R, +,.)$ is a ring.

Ring with unity.

$$(a, b)\ .\ (1, 0)=(a.\ 1-b\ .\ 0,\ b\ .\ 1+a\ .\ 0)=(a,\ b)$$

$\forall\ (a, b) \in R.$

Similarly $(1, 0)\ .\ (a, b)=(a, b)\ \forall\ (a, b) \in R.$

Hence $(1, 0)$ is the unity of $(R, +,.)$.

Commutative ring.

$$(a, b)\ .\ (c, d)=(ac-b\,l,\ bc+ad)=(ca-db,\ cb+da)$$
$$=(c\ ,\ d)\ .\ (a, b).\qquad \because\quad a\ .\ b=b\ .\ a\ \forall a, b \text{ real.}$$

Hence it is a commutative ring.

All non zero elements are inversible.

Let (a, b) where both a and b are not zero be any non zero element of R.

Suppose (p, q) is the inverse (multiplicative) of (a, b) then by def. $(a\ ,\ b)\ .\ (p, q)=$ unity of ring $=(1, 0)$

$$\therefore\quad (ap-bq,\ bp+aq)=(1, 0).$$
$$\therefore\quad ap-bq=1,\ bp+aq=0.$$

Solving above for p and q we get

$$p=\frac{a}{a^2+b^2},\quad q=-\frac{b}{a^2+b^2}.$$

Since a and b both are not zero as such $a^2+b^2\neq 0$ and hence p and q are real so that $(p, q) \in R$. Hence every non zero element $(a, b) \in R$ has a multiplicative inverse (p, q)

i.e., $$\left(\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right).$$

Thus $(R, +, .)$ is a field.

9. *Given that $(R, +, .)$ is a ring. In R define a binary operation $\times$ by the rule $a \times b = a \,.\, b + b \,.\, a$. Prove that $(R, +, \times)$ is a commutative ring.* **(Raj. M.Sc. 69)**

Making use of the fact that $(R, +, .)$ is a ring we have to establish that $(R, +, \times)$ is also a ring which we leave as an exercise for the students.

For Commutative.

$$a \times b = a \,.\, b + b \,.\, a = b \,.\, a + a \,.\, b = b \times a.$$

$\because$ Addition is commutative in $(R, +, .)$.

Hence $(R, +, \times)$ is a commutative ring.

§ 7 Certain Theorems on fields.

Theorem 2. *The multiplicative inverse of a non zero element of a field is unique.*

Let $a \in F$ such that $a \neq 0$ and b and c be the two multiplicative inverses of a.

$\therefore$ $a.b = 1$ and $a.c = 1$. where 1 is the unity of the field *i.e.*, multiplicative identity.

$\therefore$ $a.b = a.c \Rightarrow b = c$ by cancellation law.

Similarly we can establish the following.

The zero of a field *i.e.*, additive identity is unique.

The unity of a field is unique.

The additive inverse is unique.

Theorem 3. *Every field is an integral domain.*

(Luck. 68; Kanpur M.Sc. 69; Delhi 70; Meerut M Sc. 67, 69)

Recalling the definitions of integral domain and fields both of which are commutative rings with unity we have to

establish that if every non zero element is inversible which is a property of the field then the ring is without zero divisors which is a property of integral domain.

In other words given that $a \neq 0$, a^{-1} exists

i.e., $a\,a^{-1} = a^{-1}\,a = 1$. ...(1)

To prove that $ab = 0 \Rightarrow a = 0$ or $b = 0$.

or both are zero. ...(2)

Let a and b be any two elements of F such that

$ab = 0$ and $a \neq 0$ so that a^{-1} exists.

$\therefore$ $a^{-1}(ab) = 0 \Rightarrow (a^{-1}\,a)\,b = 0$ Associative.

$\Rightarrow$ $1.b = 0 \Rightarrow b = 0$.

Similarly if we start with $b \neq 0$ *i.e.*, b^{-1} exists then we can show that $a = 0$.

Hence $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Therefore it is a ring without zero divisors and as such it is an integral domain.

Thus every field is an integral domain but the converse, is not true, *i.e.*, every integral domain is not a field For example the ring of integers is an integral domain alright but it is not a field because non zero elements are not inversible except 1 and —1 as shown earlier.

Prove that in a field unity and zero are distinct elements.

Let $a \neq 0$ be an element of the field so that a^{-1} exists and is non zero. Also $aa^{-1} = 1$ where 1 is the unity.

Again every field is an integral domain which is a ring without zero divisors. $\therefore$ $1 = aa^{-1} \neq 0$

or $a \neq 0$, $a^{-1} \neq 0$

Since $1 \neq 0$, it follows that 1 and 0 are distinct elements.

Theorem 4. *An integral domain with a finite number of elements is a field.* **(Kanpur M.Sc. Stat 70; Benares M.Sc. 65, 70; Kanpur M.Sc. 71, Meerut M.Sc. 67, 69; Raj. M.Sc. 69; Delhi 70; Meerut 67)**

Let the finite integral domain D consist of n elements. Since D is an integral domain it is a commutative ring with unity without zero divisors and in order to prove that it is a field we have to prove that every non zero element of D is inversible.

Let a be any non zero element of D and we shall show that it is inversible *i.e.*, its inverse exists and belongs to the set.

$D=\{x=0, x_1, x_2, \ldots, x_{n-1}\}$ having n elements one of which is zero and one of these must also be unity.

Consider the set

$D'=\{ax_1, ax_2, \ldots, ax_{n-1} : x_i \neq 0\}$.

$x_i \in D$ and 'a' (one of x_i's) is a non zero element of D.

The above set has $n-1$ elements all of which are distinct For if not let $ax_i=ax_j \Rightarrow a(x_i-x_j)=0$ $[a\neq 0]$

$$\Rightarrow x_i-x_j=0 \Rightarrow x_i=x_j.$$

Because D being an integral domain *i.e.* a ring without zero divisors *i.e.* $ab=0 \Rightarrow a=0$, or $b=0$ or both zero.

But $x_i=x_j$ is a contradiction because D contains n elements and D' contains $n-1$ distinct elements and these will be same as the non zero elements of D.

$\because \quad a \in D, x_i \in D \Rightarrow ax_i \in D.$

Again since D is an integral domain it must have unity and hence one of the elements of D' must be unity.

Let $ax_i=1=x_ia$, $x_i\neq 1$, $a\neq 0$.

$\because$ D is commutative.

It implies that x_i is the inverse of a, $a\neq 0$.

Thus every non zero element of D has a multiplicative inverse in it and hence the integral domain D is a field.

Theorem 5. *A finite commutative ring without zero divisors is a field* **(B H. U. 68; Meerut M. Sc. 67, 69)**

If we change the above question as under.

A finite [commutative ring, **with unity**, without zero divisors which means in short an integral domain] is a field then we have proved it above in Theorem 4.

The words **with unity** are missing in the above question. Hence we will have to establish first the existence of unity element and then show that it is the multiplicative identity and finally show that each non zero element possesses an inverse.

Let $D=\{x=0, x_1, x_2, \ldots, x_{n-1}\}$ having n elements one of which is zero be a commutative ring without zero divisors.

Let $a\neq 0 \in D$ then $ax_i \in D$.

Consider the set

$D'=\{ax_1, ax_2, \ldots, ax_{n-1}\}$ in which $x_i\neq 0$

and 'a' (one of the x_i) is a non zero element of D.

The above set has $n-1$ distinct elements for if not let

$$ax_i=ax_j \Rightarrow a(x_i-x_j)=0 \; [a\neq 0] \Rightarrow x_i-x_j=0$$

$$\Rightarrow x_i=x_j.$$

Because D being a ring without zero divisors

i.e. $ab=0 \Rightarrow a=0$ or $b=0$ or both zero.

But $x_i=x_j$ is a contradiction because D contains n distinct and D' contains $n-1$ distinct elements which are same as the non zero elements of D.

$$\because \quad a \in D, x_i \in D \Rightarrow ax_i \in D.$$

Hence $ax_1, ax_2, \ldots, ax_{n-1}$ are nothing but the $n-1$ distinct non zero elements of D in some order and hence one of these elements must be equal to a as $a \in D$.

$$\therefore \quad ax_i=a=x_ia. \qquad \text{[commutative]}$$

The above is possible only if $x_i=1$ and it belongs to D.

Thus we establish the existence of element 1 in D.

Now we shall show that 1 is the multiplicative identity.

If $b \in D$ then for some $x_i \in D$, $ax_i=b=x_ia$. .. (1)

Now $1.b = 1.(ax_i)$ by (1) $= (1.a)\, x_i$. Associative

$= ax_i \quad \because \quad 1.a = a.$

$= b$ by (1) $= b.1$ as D is commutative.

Since $1.b = b = b.1$ as such 1 is the unit element of the ring.

Hence a finite commutative ring without zero divisors being a ring with unity as shown above is an integral domain.

Now we have to establish that all the non zero elements of D *i.e.* elements of D' which contain non zero elements of D are inversible.

Since all the elements of D' are again one or other non zero elements of D in some other order therefore one of these must be 1 which we have established belongs to D.

$\therefore \quad ax_i = 1 = x_i a. \quad a \neq 0,\ x_i \neq 0$

as D is commutative.

Above relation shows that $a \neq 0$ is the multiplicative inverse of non zero element x_i of D.

Hence D is a field.

Alternative definition of an Integral domain.

From above we conclude that a finite commutative ring without zero divisors is an integral domain.

Note. **An important property of a field.**

A field is closed for the four fundamental operations of addition, subtraction, multiplication and divison.

Let a and b be any two elements of the field $(F, +, .)$ then $a+b \in F$ as it is an additive group.

Also $\forall\ b \in F, \exists -b$ the add tive inverse belonging to F

$\therefore \quad a+(-b) \in F$ *i e.*, $a-b \in F$.

Also $ab \in F$ as multiplication is a binary operation

Again in a field every non zero element is inversible and belongs to F.

i.e., $\quad b \neq 0,\ b^{-1} \in F$ and $a \in F \Rightarrow ab^{-1} \in F$.

Hence the field is closed for the above four operations.

§ 8. Division ring or a skew field.

Defination. *A ring* $(R, +, .)$ *having at least two elements is called a skew field or a division ring if it is a ring with unity and is such that every non-zero element has a multiplicative inverse belonging to it.* **(Benares 63; Kanpur M. Sc. State 69)**

Comparing the definition of skew field with that of the field we find that skew field differs from the field in the sense that it is a non commutative ring, *i.e.* multiplication is not commutative.

Therefore we can define field as commutative skew field.

Ex. 1. *Prove that the set of all* 2×2 *matrices of the form* $\begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix}$ *where a, b, c, d are arbitrary real numbers form a division ring which is not a field.* **(Delhi 70)**

As proved earlier in Ex. 3 P. 172 we can show that the set of matrices is a ring and has a unity element.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ i.e. } \begin{bmatrix} 1+0i & 0+0i \\ -0+0i & 1-0i \end{bmatrix}$$

we have to see that all non zero elements are inversible.

Let the given matrix be any non zero element of the ring and $\triangle$ be its determinant then

$$\triangle = \begin{bmatrix} a+ib & c+id \\ -c+id & a-ib \end{bmatrix} = a^2+b^2+c^2+d^2$$

Now $\triangle = 0$ if and only if $a=0$, $b=0$, $c=0$, $d=0$ and in that case the element will be a zero element. Hence if the element chosen is non zero then its determinant is not zero, *i e.* it is non singular matrix and as such its inverse must exist. Hence we establish that all non zero elements are Inversible. Also we know that matrix multiplication is

not commutative and as such it is not a field but is a skew field *i.e.* a divison ring.

Point out the distinct and common properties of integral domains, fields and divison ring.

(Kanpur)

Property	I. D.	Field	Divison ring
At least two elements	Yes	Yes	Yes.
Ring with unity	Yes	Yes	Yes
Commutative	Yes	Yes	No
Without zero divisors	Yes	Yes	Yes.
(Every field is an integral domain and hence without zero divisors)			
Cancelation law holds	Yes	Yes	Yes
All non-zero elements have multiplicative inverse	—	Yes	Yes
Non-zero elements forme group w.r.t. multiplication	—	Yes but abelian	Yes but not abelian.

§ 9. Isomorphism of two rings.

Two rings R and R' are said to be isomorphic to each other if there exists one-one onto mapping $f : R \to R'$ such that

$$f(a+b)=f(a)+f(b), \text{ and } f(a.b)=f(a).f(b),$$
$$\forall\ a, b \in R.$$

and we write it as $R \cong R'$. and R' is called isomorphic image of R

This mapping f is then said to be isomorphism of R onto R', *i.e.* a mapping which is one-one onto and preserves the two compositions of the ring.

§ 10. Theorems on Isomorphism of rings

If f is an isomorphism of a ring R onto a ring R' such that $f(a+b)=f(a)+f(b)$ .. (1)

$f(a.b)=f(a).f(b) \ \forall\ a, b, \in R,$ ...(2)

then prove the following.

Theorem A. The image of the zero of R is zero of R′.
See § 17 P. 108 of Groups

Since f is one-one-onto mapping hence corresponding to any element a' of R' $\exists$ an element $a \in R$ such that $f(a)=a'$

Let 0 be the additive identity of R then $f(0)=0'$ say $\in R'$ we shall show that 0′ is the additive identity of R'.

Now $a+0=a=0+a$.
$\therefore$ $f(a+0)=f(a)=f(0+a)$
$\therefore$ $f(a)+f(0)=a'=f(0)+f(a)$
or $a'+0'=a'=0'+a' \ \forall \ a' \in R'$
Hence 0′ is the identity of R'
But $0'=f(0)=$identity of R'
$\therefore$ Image of identity 0 of R is the identity of R'

Theorem B. The image of the additive inverse (i.e. negative) of an element a of R is the additive inverse (i.e. negative) of the image of that element.

Let $a \in R$ and $-a$ be its additive inverse in R so that $a+(-a)=0=(-a)+(a)$ where 0 is the identity of R
$\therefore$ $f[(a+(-a)]=f(0)=f[(-a)+a]$
or $f(a)+f(-a)=0'=f(-a)+f(a)$ where 0′ is the identity of R' by (*A*)

Above relation shows that $f(-a)$ is the additive inverse of $f(a) \in R'$
$\therefore$ $f(-a)=-f(a)$
i.e. image of the additive inverse of an element is the additive inverse of the image of that element.

Theorem C. The isomorphic image of a commutative ring R is also a commutative ring R′.

Let $a, b \in R$ so that $ab=ba$ as R is commutative
$\therefore$ $f(a)$ and $f(b) \in R'$.

Now $f(a)\, f(b)=f(ab)=f(ba)=f(b)\, f(a)$

Hence R' is also a commutative ring.

Theorem D. Isomorphic image of a ring R with unity is a ring R′ with unity.

Let 1 be unity element of R so that $f(1) \in R'$

Now $a.1=a=1.a$, where $a \in R$ and $f(a) \in R'$

$$f(a).f(1)=f(a.1)=f(a).$$

$$f(1).f(a)=f(1.a)=f(a).$$

Hence $f(a)\, f(1)=f(a)=f(1)\, .f(a)$ where $f(a), f(1) \in R'$

Above relation shows that $f(1) \in R'$ is the unity element of R'.

Theorem E. The isomorphic image of a ring without zero divisors is a ring without zero divisors.

Ring without zero divisors $a\neq 0, b\neq 0 \Rightarrow ab\neq 0$

Let $f(a)$ and $f(b)$ be two non zero elements of R'

So that a and b are also non zero elements of R as by 1 zeros of R and R' correspond.

Now $f(a).f(b)=f(ab)\neq f(0)$. as $ab\neq 0$

or $f(a)\, f(b) \neq 0'$ where $0'=f(0)$ is the zero of R'

or $a'b' \neq 0'$ where a', b' are two non zero elements of R'.

Therefore R' is also a ring without zero divisors.

Theorem F. Isomorphic image of an integral domain is an integral domain.

Integral domain is a commutative ring with unity without zero divisors and hence by C, D, E above its isomorphic image is also a commutative ring with unity and without zero divisors and as such it is an integral domain.

Theorem G. Isomorphic image of a field is a field.

Let R be a field so that it is a commutative ring with unity such that each non zero element is inversible. Now by

C and D the isomorphic image of R *i e.* R' will also be a commutative ring with unity and $f(1)$ will be its unit element. **(It is given that R′ is a ring)**

Let $a \neq 0 \in R$ so that a^{-1} exists such that $a\,a^{-1} = a^{-1}a = 1$.

Agian let $f(a)$ be any non zero element of R' so that $a \neq 0 \Rightarrow a^{-1}$ exists $\Rightarrow a\,a^{-1} = a^{-1}\,a = 1$

Now $f(a)\,f(a^{-1}) = f(a\,a^{-1}) = f(1) =$ unit element of R'

$f(a^{-1})\,f(a) = f(a^{-1}\,a) = f(1) =$ unit element of R'

Above relation shows that each non zero element $f(a) \in R'$ is inversible *i.e.* possesses a multiplicative inverse. Hence R' is a field.

Theorem H. Isomorphic image of a division ring is a division ring.

Division ring is a ring with unit element such that every non zero element is inversible and hence by D and G its isomorphic image is also a division ring.

We can also say that because every field is a division ring and hence by G the theorem follows.

Theorem 6. *The relation of isomorphism in the set of all rings is an equivalence relation.*

Let R_1, R_2, R_3 be elements of the set of rings. In order to prove that the relation of isomorphism is an equivalence relation we have to show that it is **reflexive, symmetric and transitive.**

(1) **Reflexive.** To prove that $R_1 \cong R_1$. This is clearly true because there exists an identity mapping I of R_1 onto itself which is an isomorphism.

$\because \quad I(a+b) = a+b = Ia+Ib,\ I(ab) = ab = I(a).I(b)$

Symmetric. If $R_1 \cong R_2$ then $R_2 \cong R_1$ *i.e*, $\exists$ a one-one onto mapping from R_2 to R_1 which preserves the two ring compoisitions.

Now $R_1 \cong R_2 \Rightarrow \exists\ a$ a mapping $f : R_1 \to R_2$ which is one-one onto and preserves ring compositions.

Since f is one-one-onto $\Rightarrow \exists$ a mapping $f^{-1} : R_2 \Rightarrow R_1$ which is also one-one-onto. The only thing we have to show now is that f^{-1} also preserves ring compositions.

Let a_2, b_2 be any two elements of R_2, then
$f^{-1}(a_2) = a_1, f^{-1}(b_2) = b_1$ where $a_1, b_1 \in R_1$.
$\therefore \quad f(a_1) = a_2, f(b_1) = b_2$ ...(1)
Now $f^{-1}(a_2 + b_2) = f^{-1}(f(a_1) + f(b_1))$
$= f^{-1}(f(a_1 + b_1))$ $\because f : R_1 \to R_2$ is an isomorphism
$= a_1 + b_1 = f^{-1}(a_2) + f^{-1}(b_2)$.

Again $f^{-1}(a_2\ b_2) = f^{-1}(f(a_1).f(b_1))$
$= f^{-1}(f(a_1\ b_1))$ $\because f : R_1 \to R_2$ is an isomorphism.
$= a_1\ b_1 = f^{-1}(a_2)\ f^{-1}(b_2)$. ...(3)

From (2) and (3) we conclude that f^{-1} preserves the ring compositions and hence $f^{-1} : R_1 \to R_2$ is an isomorphism.

Transitive. Let R_1, R_2, R_3 be any three rings such that $R_1 \cong R_2$ and $R_2 \cong R_3$ so that $\exists$ isomorphic mappings $f : R_1 \to R_2$ and $g : R_2 \to R_3$. We have to show that $R_1 \cong R_3$ *i.e.* $\exists$ an isomorphic mapping from R_1 onto R_3.

Now both f and g are one-one-onto mappings therefore the composite mapping $g\ f$ is also one one-onto where $g f : R_1 \to R_3$.

Now $g f(a+b) = g[f(a+b)] = g[f(a) + f(b)]$
$\because$ f is an isomorphism.
$= g[f(a)] + g[f(b)]$ $\because$ g is an isomorphism.
$= (g f)\ a + (g f)\ b$.

Again $g f(ab) = g[f(ab)] = g[f(a).f(b)]$. As above.
$= g[f(a)[.g[f(b)]$
$= (g f)\ a.(g f)\ b$

Hence $g\,f$ preserves the ring compositions and it being one-one-onto is therefore an isomorphism.

Therefore the relation of isomorphism in the set of all rings is an equivalence relation. It will partition the set of all rings into mutually disjoint classes such that any two rings of the same class are isomorphic to each other whereas the rings of different classes are not isomorphic. Any two rings belonging to the same equivalence class are said to be **abstractly identical.**

Ex. 1. *Prove that the isomorphic image of a field is a field.*

The students may feel as to why this example is given again here when we have proved in part *G* above. The difference here is that in *G* it was given that f is an isomorphism of a ring R onto a ring R'. Here R' is the isomorphic image of R which is a field and we will have to prove first that R' is a ring.

The element of R' are $f(a), f(b), f(c)$

where $a, b, c \in R$

Such that $f(a+b)=f(a)+f(b)$ ...(1)

$f(ab)=f(a)\,f(b)$ .. (2)

R′ is a ring :

(1) **R′ is closed for addition.**

$a, b \in R \Rightarrow a+b \in R \Rightarrow f(a+b) \in R'$,

$f(a), f(b \in R'$

$\therefore\ f(a)+f(b)=f(a+b) \in R'$. Thus R' is closed for addition.

(2) Addition is associative in R'

$[f(a)+f(b)]+f(c)=f(a+b)+f(c)$. by 1

$=f[(a+b,+c]=f(a+(b+c)]$ $\because$ R is a ring.

$=f(a)+f(b+c)=f(a)+[f(b)+f(c)]$

Hence associative.

(3) **Identity exists.** $f(0)$ is the identity **See A, P. 211**

(4) **Additive inverse exists.** $-f(a)$ is the additive inverse of $f(a) \in R'$ **See B. P. 211**

(5) **Addition is commutative.**

$$f(a)+f(b)=f(a+b)=f(b+a)=f(b)+f(a)$$

$\because$ $a+b=b+a$ in R.

R_2. Multiplication is a binary composition which is associative.

$a, b \in R \Rightarrow ab \in R$. Also $f(a), f(b), f(ab) \in R'$

Now $f(a)\,f(b)=f(ab)$ by (2) $\in R'$

Hence R' is closed for multiplication.

Again $[f(a)\,f(b)]\,f(c)=f(ab).\,f(c)=f[(ab)\,c]$

$=f[a\,(bc)]$ $\because$ R is a ring.

$=f(a)\,f(bc)=f(a)\,[f(b).\,f(c)]$

Hence multiplication is associative.

R_3. Right and left distributive Laws hold.

$a.(b+c)=a.b+a.c$, $(a+b).c=a.c+b.c$

as R is a field.

$\therefore$ $f[(a.(b+c)]=f[(a.b+a.c]$

or $f(a)\,f(b+c)=f(a.b)+f(a.c)$

or $f(a).[f(b)+f(c)]=f(a).\,f(b)+f(a).\,f(c)$

Above shows that right distributive law holds in R' and similarly we can prove the left distributive law.

Therefore R' is a ring.

Now since R is a field *i.e.* a commutative ring with unity such that all non zero elements are inversible. Therefore R' is also a commutative ring with unity in which all non zero elements are inversible as proved in *C*, *D* and *G*.

Ex. 2. *Let R be a ring $(R, +, .)$ of integers and R' be the set of all even integers with an operation denoted by* $*$

defined as $a*b=\frac{ab}{2}$ *where ab is the ordinary multiplication of a and b then prove the following.*

(*a*) $(R', +, *)$ *is a commutative ring.*

(*b*) $R \cong R'$

(*c*) *What acts as the unit element of* R'.

(a) It is easy to prove that, R' is an abelian group under ordinary addition. Let a and $b \in R$ so that a and b both are even so that $a*b=\frac{a\,b}{2}$=even and as such the set R' is closed for the operation.

Again if $a, b, c \in R'$ then $a*(b*c)=a*\left(\frac{b}{2}\frac{c}{}\right)=\frac{a(bc/2)}{2}$

$$=\frac{(a\ b/2)\ c}{2}=\left(\frac{ab}{2}\right)*c=(a*b)*c$$

$\therefore$ The operation * is associative.

Again $a*b=\frac{ab}{2}=\frac{ba}{2}=(b*a)$ and hence commutative.

Distributive Law $a*(b+c)=\frac{a\,(b+c)}{2}=\frac{ab}{2}+\frac{ac}{2}$

$$=(a*b)+(a*c)$$

Similarly $(a+b)*c=a*c+b*c$.

$\therefore$ $(R', +, *)$ is a commutative ring.

(*b*) $R \cong R'$. Let $f: R \to R'$ such that $f(x)=2x$

$$\forall\ x \in R,\ 2x \in R'$$

This mapping is clearly one-one-onto.

$f(m+n)=2(m+n)=2m+2n=f(m)+f(n)\ \forall\ m, n \in R$

$f(mn)=2mn=\frac{2m.2n}{2}=2m*2n=f(m).f(n)$

$\therefore$ f preserves the two operations.

$\therefore$ $R \cong R'$.

(e) 1 is the unity element of R $\therefore$ $f(1)=2$ by def. of f.

$\therefore$ $f(1)=2$ is the unity element of R' as f is an isomorphism.

and $a*2=\frac{a.2}{2}=a=2*a$. $\therefore$ 2 is the unity of R'.

§ 11. Transference of Rings Structure.

Theorem. *If f is a one-one mapping of a ring R onto a set R' with two compositions denoted additively and multiplicatively such that*

$f(a+b)=f(a)+f(b), f(ab)=f(a)f(b)$ $\forall$ $a, b, \in R$.

then the set R' is a ring for the two compositions.

(Benares 67)

We can prove the above theorem exactly in the manner we proved the corresponding theorem in groups in §18 P. 112.

§ 12. Sub rings.

Let $(R, +,.)$ be a ring and S be a sub set of R. If the sub set S is closed for both the compositions $+$ and $.$ then the set S forms a ring for these two compositions and is called a sub ring. It is obvious that in this case S will be a sub group of the additive group $(R, +)$ of ring $(R, +, .)$

In other words $a, b \in S \Rightarrow a+b \in S$ and $ab \in S$ or S is stable for the two operations. **(Kanpur M. Sc. 69)**

$\{0\}$ and R always sub rings of R known as **improper sub rings** of R.

§ 13. Theorems on Sub Rings

Theorem 7. *A non empty sub set S of a ring $(R, +,.)$ will form a ring if and only if*

(*i*) $a-b \in S$ $\forall$ $a, b \in S$.

(*ii*) $ab \in S$ $\forall$ $a, b \in S$. **(Meerut B. Sc. 69)**

Ist Case. S is a sub ring.

Since S is a sub ring so the set $(S, +)$ is an additive sub

group of $(R, +)$ and consequently

$$a \in S, b \in S \Rightarrow a-b \in S.$$

Also S being a sub ring it is closed for multiplication by definition

$$\therefore \quad a \in S, b \in S \Rightarrow ab \in S.$$

Converse. Given $a-b \in S$, $ab \in S \ \forall \ a, b \in S$ to prove that $(S, +, .)$ is a ring *i.e.*, a sub ring

R_1 **$(S, +)$ is an additive abelian group**

$a \in S, a \in S \Rightarrow a-a \in S$ *i.e.* $0 \in S$ **Identity.**

$0 \in S, a \in S \Rightarrow 0-a \in S$ *i.e.* $-a \in S$ **Inverse.**

$b \in S$ then $-b \in S$ as shown above

$\therefore \quad a \in S, -b \in S \Rightarrow a-(-b) \in S \Rightarrow a+b \in S$ closed.

Again addition is both associative and commutative as it is so in R.

R_2 Multiplication is a binary operation as

$$a \in S, b \in S \Rightarrow ab \in S$$

and it is associative because this property holds in R.

R_3 Multiplication distributes addition as it holds in R.

Thus all the ring postulates are satisfied. Hence S is a ring or a sub ring of R.

Theorem 8. *The intersection of two sub rings is a sub ring.*

Let S and T be two sub rings and we have to show that $S \cap T$ is also a sub ring.

Let $a, b \in S \cap T$ then we show that

$$a-b \in S \cap T \text{ and } ab \in S \cap T$$

and as such it will form a sub ring by Theorem 7.

Now $\quad a \in S \cap T \Rightarrow a \in S, a \in T.$

$$b \in S \cap T \Rightarrow b \in S, b \in T.$$

Now $\quad a \in S, b \in S \Rightarrow a-b \in S, ab \in S$

$\because$ S is a sub ring.

Also $a \in T, b \in T \Rightarrow a-b \in T, ab \in T$

$\because$ T is a sub ring

$\therefore$ $a-b \in S, a-b \in T \Rightarrow a-b \in S \cap T$.

Also $ab \in S$, $ab \in T \Rightarrow ab \in S \cap T$.

Therefore $S \cap T$ is also a sub ring.

Generalising the above theorem we can say that the intersection of any arbirary family of sub rings is also a sub ring. **(Raj. M.Sc. 69)**

Prove as in § 22 P. 122.

Theorem 9. *The necessary and sufficient condition for a non empty sub set S of a ring R to be a sub ring of R are*

(*i*) $S+(-S)=S$ (*ii*) $SS \subseteq S$.

(Meerut B.Sc. Summer 70)

Case I. Given S is a sub-ring. To prove i and ii

Since S is a sub-ring as such S is sub-group of additive group of ring R.

Let $a+(-b)$ be any element of $S+(-S)$

$\Rightarrow$ $a \in S, -b \in -S$

$\Rightarrow$ $a \in S, b \in S \Rightarrow a-b \in S$ $\because$ S is a sub-group.

$\therefore$ $S+(-S) \subseteq S$ ...(1)

Again $a \in S$ which is a sub-group and $0 \in S$ or $\in -S$.

$\therefore$ $a=a+0 \in S+(-S)$

$\therefore$ $S \subseteq S+(-S)$. ...(2)

Hence from 1 and 2 we get $S+(-S)=S$. Thus (i) is proved.

Again since S is a sub-ring it must be closed for multiplication.

$\therefore$ $a \in S, b \in S \Rightarrow ab \in S$.

But ab is any element of $SS \Rightarrow ab \in S$ by above

$\therefore$ $SS \subseteq S$. Hence (ii) is proved.

2nd Case. Given (i) $S+(-S)=S$ **(ii)** $SS \subseteq S$.

To prove. S is a sub-ring *i.e.* $ab \in S$, $a-b \in S$
$\forall\ a, b \in S$ Th. 7

$\forall\ a, b \in S$, $ab \in S\ S \Rightarrow ab \in S \because S\ S \subseteq S$

Again $S+(-S)=S \Rightarrow S+(-S) \subseteq S$.

$\Rightarrow a+(-b) \in S\ \forall\ a, b \in S$

$\Rightarrow a-b \in S\ \forall\ a, b \in S$.

Hence $\forall\ a, b \in S$ we have $a-b \in S$, $ab \in S$, therefore S is a sub-ring by Theorem 7.

Exercise 4

Ex. 1. *Prove that the set* S *of* 2×2 *matrices* $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ *is a sub-ring of a ring of* 2×2 *matrices.* **(Meerut B Sc. 69)**

Let $A=\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$, $B=\begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$ be any two elements of S.

Then $A-B=\begin{bmatrix} a_1-a_2 & b_1-b_2 \\ 0 & c_1-c_2 \end{bmatrix}$ which is again an element of S.

Also $AB=\begin{bmatrix} a_1a_2 & a_1b_2+b_1c_2 \\ 0 & c_1c_2 \end{bmatrix}$ which is again an element of S.

Then $\forall\ A, B \in S$ we have $AB \in S$ and $A-B \in S$, hence S is a sub ring by Th. 7.

In a similar manner we can prove that the set S of matrices of the type $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ is a sub ring of the ring of 2×2 matrices.

Ex. 2. *The set of all* $n\times n$ *matrices over the field of rational numbers is a sub ring of the ring of all* $n\times n$ *matrices over the field of real numbers.*

Ex. 3. *The set of integers is a sub ring of the set of the ring of rational numbers.*

Ex. 4. *The set of even integers is a sub ring of the set of the ring of integers.*

Ex. 5. *$(R, +, .)$ be a ring of integers. For any fixed integer m let $S=\{\ldots -3m, -2m. -m, 0, m, 2m, 3m \ldots\}$ then S is a sub ring of R.*

Let $a=mp$, $b=mq$ be any two elements of S where p, q are integers.

Then $a-b=mp-mq=(p-q)\ m=km$ where k is an integer.

$ab=mp.mq=(mpq)m=lm$ where l is an integer.

Thus $\forall\ a, b \in S, a-b$ and ab both $\in S$ and hence S is a sub ring by Th. 7.

6. *If R is a ring show that*

$Z(R)=\{x \in R : xy=yx\ \forall\ y \in R\}$ is a subring of R what happens to $Z(R)$ if R is a divison ring

Let $x_1, x_2 \in Z(R)$

$\therefore\quad x_1 y=y x_1, x_2 y=y x_2 \qquad \forall\ y \in R \qquad \ldots(1)$

$(x_1-x_2)\ y=x_1y-x_2y=y x_1-y x_2=y(x_1-x_2)\ \forall\ y \in R$

$\therefore\quad x_1-x_2 \in Z(R) \qquad \ldots(2)$

Again $(x_1 x_2)\ y=x_1(x_2 y)=x_1(y x_2)=x_1 y)\ x_2=(y x_1)\ x_2$

$=y(x_1 x_2)\ \forall\ y \in R$

Hence $x_1 x_2$ also $\in Z(R) \qquad \ldots(3)$

From (2) and (3) we find that the criteria for a sub-ring are satisfied $\quad\therefore\quad Z(R)$ is a sub ring.

Again as $1 . y=y . 1 \quad \forall\ y \in R$ therefore $1 \in Z(R)$ *i.e.* $Z(R)$ is a ring with unity which is commutative by definition.

In case R is a division ring then by definition multiplicative inverse of each non-zero element exists in R

Now $x \in Z(R)$ then $xy=yx\ \forall\ y \in R$

$\Rightarrow\ x^{-1}(xy)\ x^{-1}=x^{-1}(yx)x^{-1} \quad \forall\ y \in R$

$\Rightarrow\ (x^{-1}x)(yx^{-1})=(x^{-1}y)(x\ x^{-1})\ \forall\ y \in R$

$$\Rightarrow yx^{-1}=x^{-1}y \quad \forall\ y \in R$$
$$\Rightarrow x^{-1} \in Z(R)$$

Thus multiplicative inverse of all non-zero x in $Z(R)$ exists in $Z(R)$ and we have already shown that $Z(R)$ is a commutative ring with unity

Hence $Z(R)$ is a field

§ 14. Sub Field.

Def. *A sub set S of a field $(F, +.)$ is said to be a sub field if F is closed with respect to addition and multiplication in F and is itself a field for these two compositions.*

Theorem 10. *A sub set S of a field $(F, +, .)$ consisting of at least two elements is a sub field if and only if*

(i) $a \in S, b \in S \Rightarrow a-b \in S$

(ii) $a \in S, b \in S\ (b \neq 0) \Rightarrow ab^{-1} \in S$. **(Bombay 70)**

Proof :

1st Case. Given. S is a sub field. To prove (i) and (ii).

Since S is a field it is a sub group of the additive group of the field F.

$\therefore$ $a \in S, b \in S \Rightarrow a-b \in S$, which proves (i).

Again since S is itself a field therefore each non zero element of S is inversible.

Let $b \neq 0 \in S \Rightarrow b^{-1} \in S$.

$\therefore$ $a \in S, b^{-1} \in S$ and S is closed for multipiication.

$\therefore$ $ab^{-1} \in S$ which proves (ii).

2nd Case. Given S is a sub set of F such that

$\forall\ a, b \in S, a-b \in F$ and $ab^{-1} \in S\ (b \neq 0)$.

To prove that S is a sub field.

$(S, +)$ is an additive abelian group.

$a \in S, a \in S \Rightarrow a-a \in S \Rightarrow 0 \in S$. Identity

$0 \in S, a \in S \Rightarrow 0-a \in S \Rightarrow -a \in S$ Inverse

$b \in S$ then $-b \in S$ as shown above.

$\therefore \quad a \in S, -b \in S \Rightarrow a-(-b) \in S \Rightarrow a+b \in S.$

$\therefore$ S is closed for addition.

Again addition is both associative and commutative as it is so in $(F,+,.)$.

Multiplication is associative cmmutative and distribtes addition as all these hold in $(F, +, .)$. We will prove in the end that multiplication is a binary operation.

Existence of Unity. Let a be any non zero element of S then by (ii)

$$a\, a^{-1} \in S \Rightarrow 1 \in S.$$

Existence of multiplicative inverse of each non zero element.

$1 \in S$, and let $a \neq 0 \in S \Rightarrow 1.a^{-1} \in S \Rightarrow a^{-1} \in S$.

Closed for multiplication *i.e.* **binary operation.**

Let $b \neq 0 \in S \Rightarrow b^{-1} \in S$.

Now let $a \in S, b^{-1} \in S \Rightarrow a\,(b^{-1})^{-1} \in S$ by (ii)

$$\Rightarrow ab \in S$$

Again if $b=0$ then $ab=0$ and $0 \in S \therefore ab \in S$.

Hence $\forall\ a, b \in S\ ab \in S$.

Illustration. We know that the set R of real numbers is a field of which the set Q of rational numbers is a sub field for addition and multiplication. Similarly the set C of com plex numbers is a field of which the set R of real numbers is a sub field for the same compositions.

§ 15 Ordered integral domain.

An integral domin $(I, +, .)$ is said to be an ordered integral domin if I contains a sub set S with the following properties.

(1) $a+b \in S\ \forall\ a, b \in S$

i.e., closed under addition.

(2) $ab \in S\ \forall\ a, b \in S$

i.e., closed under multiplication.

(3) For every $a \in I$ only one of the following is true $a=0$, $a \in S$, $-a \in S$. (Trichotomy Law).

(Allahabad 65; Bombay 70)

The elements of the set S are called the positive elements of I. A **field** $(F, +, .)$ is said to be ordered if it is ordered as an integral domain.

Exercise 5

1. *The integral domain* $(I, +, .)$ *of all integers is ordered because* I *contains a set* S *of all* $+ive$ *integers which satisfy the above properties i.e., sum and product of two* $+ive$ *integers is again a* $+ive$ *integer. Also if* $a \in I$ *then either* a *is* $+ive$ *or* $-ive$ *or,* 0 *i.e., either* $a \in S$ *or* $-a \in S$ *or* $a=0$.

Similarly the integral domain of all rational numbers is ordered integral domain. The integral domain of all real numbers is ordered integral domain.

2. *Prove that the integral domain* $(C, +, .)$ *of complex numbers is not ordered.* **(Allahabad 67, 70)**

Let us suppose that it is an ordered integral domain S be the set of $+$ive elements of C then the elements of S will be closed both for addition and multiplication and for every element $a \in C$, only one of the following is to hold good

i.e., $a=0$ or $a \in S$ or $-a \in S$.

Now i is any element of C which is not zero then by above property either $i \in S$ or $i \in S$.

Let us choose that $i \in S$ then $i.i \in S$ or $-1 \in S$ by property 2.

Again $i \in S$, $-1 \in S \Rightarrow i(-1) \in S \Rightarrow -i \in S$ by property 2.

But this is not possible because both i and $-i$ can not belong to C by third property of definition of ordered I. D.

3. *Show that the field*

$$F=\{0, 1, 2, 3, 4, +_5, \times_5\}$$

is not ordered. **(Allahabad 70)**

Let S be the set of +ive elements of F, *i.e.* $S=\{1, 2, 3, 4\}$ then $\forall\ a, b \in S\ a+b \in S$ under addition modulo 5

$\forall\ a, b, \in S \quad ab \in S$ under multiplication modulo 5

Let us choose $a=1$ then its inverse $-a$ is 4 under addition modulo 5 as $1 \underset{+5}{+} 4=0$ (*i.e.* identity).

Now $a\neq 0$, *i.e.* $1\neq 0$, but since both 1 and its inverse $4 \in S$ therefore the third condition of ordered integral domain is violated. Hence it is not an ordered field.

Order relations in an ordered integral domain.

Definition Let $(D,+, .)$ be an integral domain and D_+ be the set of +ive elements of D, then we define less than $<$ and greater than $>$ relation in D as under.

(1) $a > b$ when $a-b \in D_+ \quad \forall\ a, b \in D$

(2) $a < b$ when $b-a \in D_+ \quad \forall\ a, b \in D$

Clearly $a < b \Leftrightarrow b>a$.

The order relation is transitive in an ordered I D.

$a>b \Rightarrow a-b \in D_+$

$b>c \Rightarrow b-c \in D_+$

But D_+ is closed for addition by definition of ordered I.D.

$\therefore \quad (a-b)+(b-c) \in D_+ \Rightarrow a-c \in D_+$

$\Rightarrow a>c$

Thus $a>b, b>c \Rightarrow a>c$. Hence **proved.**

4. *Show that the unity element* 1 *of an ordered integral domain D is a positive element of D.* **(Allahabad B.Sc. 66)**

Let if possible $1 \notin D_+$ where D_+ stands for the set of all +ive elements of D. Also $1\neq 0$

Now by third property of ordered integral domain, only one of the following is true

i.e. $a=0$, $a \in S$, $-a \in S$ where a is a sub set of ordered I.D.

Now D_+ is a sub set of D

and $1 \neq 0$, $1 \notin D_+$ therefore $-1 \in D_+$

$\therefore$ (-1) $(-1) \in D_+$ by prop. 2 § 15.

$\Rightarrow 1 \in D_+$ which is a contradiction to our supposition that $a \notin D_+$. Hence $1 \in D_+$.

§ 16. Divisibility in an integral domain.

If a and b be two non zero elements of an integral domain I.D. and if there exists an element $c \in$ I.D., such that $b=ac$ then a is said to be a divisor of b or a is a factor of b or b is divisible by a and we express it as a/b, *i.e.* a divides b so that $b=ac$. In the integral domain $(I, +, .)$ $4/12$ as $12=4.3$ and $3 \in I$. Similarly in I.D. $(Q, +, .)$ $4/7$ as $7=4.7/4$ and $7/4 \in Q$.

Theorem 11. *The relation of divisibility in an integral domain is reflexive as well as transitive.* **(Allahabad 67)**

Reflexive. $a=a.1$, $\therefore$ a/a, *i.e.* a divides a.

Transitive. Let a/b and b/c, $a \neq)$, $b \neq)$, *i.e.* a divides b and b divides c, both a and b are non zero.

$a/b \Rightarrow b=ap$, $b/c \Rightarrow c=bq$, $p, q \in$ I.D.

$\therefore$ $b=ap$ and $c=bq \Rightarrow c=(ap)\, q=a\,(pq)$, $pq \in$ I.D.

The above relation implies that a divides c, *i.e.* a/c.

$\therefore$ a/b, $b/c \Rightarrow a/c$, $\therefore$ Transitive.

1. *In the integral domain of Gaussian integers* $a+ib$: $a, b \in I$, *we have*

$$(2+3i)\,(4+5i)=-7+22i.$$

We can say that $4+5i$ divides $-7+22i$ *i.e.*

$$(4+5i)/(-7+22i).$$

Similarly we can say $2+3i$ divides $-7+22i$. *i.e.*

$$(2+3i)/(-7+22i).$$

2. *In an integral domain* $(I, +, .)$ *prove the following*

(*a*) $a/b, a/c \Rightarrow a/(b+c)$ (*b*) $a/b \Rightarrow a/bx \ \forall\ x \in$ I.D.

$a/b \Rightarrow b=ap, a/c \Rightarrow c=aq, p, q \in$ I.D.

$\therefore\ b+c=ap+aq=a(p+q)=ar, r \in$ I.D.

$\therefore\ a/(b+c).$

(*b*) $a/b \Rightarrow b=ap \Rightarrow bx=a\,px \Rightarrow bx=a(px)=ar$

where $r \in$ I.D.

$\therefore\ a/bx.$

§ 17. Units and Associates in an integral domain.

Units. *All the elements of an integral domain which have their multiplicative inverses in D are called its units.*

From definition we observe that if $a \in D$ and it is inversible then $a^{-1} \in D$ such that $aa^{-1}=1$. In other words a divides 1, *i.e.* $a/1$.

In the integral domain of integers the only inversible elements are 1 and -1 which therefore are its units. In a field all the non zero elements are inversible and as such all of them are units. Also from the definition it is clear that if a is unit then a^{-1} is also a unit. Again if a and b are two units. *i.e.* they are inversible then their product ab is also inversible *i.e.* $(ab)^{-1}=b^{-1}a^{-1}$ which $\in D$ as both a^{-1} and $b^{-1} \in D$.

Students should have no confusion between units and unity. The unity is unique, whereas the units may be many.

3. *Prove that* $1, -1, i, -i$ *are the only four units in the integral domain of gaussian integers.*

Let $a+ib$ be a unit of the I D. of gaussian integers and $c+id$ be its multiplicative inverse so that

$$(a+ib)(c+id)=1$$

or $$(ac-bd)+i(bc+ad)=1.$$

$\therefore\ ac-bd=1$ and $bc+ad=0.$

Squaring and adding the above relations, we get

$$a^2c^2+b^2d^2+b^2c^2+a^2d^2=1$$

or $a^2(c^2+d^2)+b^2(c^2+d^2)=0$ or $(a^2+b^2)(c^2+d^2)=1$

a, b, c, d are all integers and the product of the +ive integers is 1 only when each of them is 1.

$$\therefore \quad a^2+b^2=1,\ c^2+d^2=1.$$

$$\therefore \quad a^2=1,\ b^2=0 \text{ or } a^2=0,\ b^2=1$$

or $$a=\pm 1,\ b=0 \quad \text{or} \quad a=0,\ b=\pm 1.$$

Putting the values of a and b we get the units as $1, -1: i, -i$.

Associates of an integral domain.

Definition. *Two non zero elements a and b of an integral domain are said to be associates if a is a divisor of b and b is a divisor of a i e. a/b and b/a or b=ap, a=bq, p, q ∈ I. D. ane it is expressed as a ~b.*

For example in the integral domain of integers any element a is an associate of itself as well as of $-a$. Thus $a, -a$, are associates. Similarly in the integral domain of gaussian integers the number $a+ib$ is an associate of each numbers

$$a+ib,\ -a-ib,\ -ia+b,\ ia-b.$$

Theorem 12. *The relation of being associates in an integral domain is an equivalence relation.*

Reflexive : We know that a/a as $a=a.1$.

$\therefore$ a is associate of itself *i.e.* $a \sim a$.

Symmetric : $a \sim b \Rightarrow a/b$ and b/a

$\Rightarrow b/a$ and $a/b \Rightarrow b \sim a$.

Transitive, Let $a \sim b$ and $b \sim c$.

Then a/b, b/a and b/c and c/b.

$\therefore$ a/b and $b/c \Rightarrow a/c$

c/b and $b/a \Rightarrow c/a$.

Hence a/c and c/a implies a is an associate of c *i.e.* $a \sim c$ and hence transitive.

Theorem 13. *Two elements a and b of an integral domain are associates if each is unit times the other.*

Proof. $a, b \in I$ be associates so that a/b and b/a.

a/b, *i.e.* a divides $b \Rightarrow b=ac$ ($c \in$ I. D.)

b/a, *i.e.* b divides $a \Rightarrow a=bd$ ($d \in$ I. D.)

$\therefore \quad a=bd=acd$ or $a.1=a.(cd)$,

where 1 is the unity.

Hence by cancellation law we get $cd=1$.

In other words c and d are multiplicative inverses of each other and all those elements whose multiplicative inverses exist are called units.

$\therefore$ $b=ac$, *i.e.* b is unit times a
$a=bd$, *i.e.* a is unit times b } c and d being units.

Converse. Let u be the unit of I. D. and that $b=ua$, *i.e.* one is unit times other then we shall show that a and b are associates, *i.e.* a/b, b/a.

Given $b=ua \Rightarrow u^{-1} b=u^{-1} ua=1.a=a$.

$\therefore \quad u^{-1} b=a \Rightarrow b$ is a divisor of a, *i.e.* b/a.

Also $b=ua$ shows that a is a divisor of b, *i.e.* a/b.

Therefore a and b are associates.

Note. From above we conclude that the associates of an element a can all be obtained by multiplying a by different units of the domain.

Fermat's theorem.

If a is an integer and p is a prime then $a^p=a \pmod p$

(B. H. U. 70; Agra 70)

From example 2. *P*. 196 $R=\{0, 1, 2, \ldots, p-1, +, .\}$ where p is prime is a finite field. Again we know that in a field all non-zero elements constitute a group for multiplication modulo p whose order is $p-1$.

Again from cor 2 P. 162 we know that order of an element of *a* finite group is a divisor of the order of the group and in particular $a^n=e$

Hence $a^{p-1}=1 \pmod p$ or $a^p=a \pmod p$.

Ex. 3. *Prove that* $\pm 1, 4\pm\sqrt{17}, -4\pm\sqrt{17}$ *are the units and* $2-\sqrt{17}$ *and* $-9-2\sqrt{17}$, *are the associates in the integral domain* $D=a+b\sqrt{17}$, $a, b \in I$.

Let $x+y\sqrt{17} \in D$ be a unit, then there exists an element $p+q\sqrt{17} \in D$ such that

$$(x+y\sqrt{17})\,(p+q\sqrt{17})=1 \text{ by definition}$$

or $$(px+17qy)+\sqrt{17}\,(qx+py)=1+\sqrt{17}.0$$

$$\therefore \quad px+17qy=1 \text{ and } qx+py=0.$$

Solving we get

$$p=\frac{x}{x^2-17y^2},\quad q=\frac{-y}{x^2-17y^2},$$

p and q both have to be integers.

$$\therefore \quad x^2-17y^2=\pm 1.$$

Hence $x+y\sqrt{17}$ is a unit if and only if $x^2-17y^2=\pm 1$ and this is possible if $x=\pm 1$, $y=0$, $x=\pm 4$, $y=\pm 1$.

Hence $\pm 1, \pm 4\pm\sqrt{17}$ are the units in D.

Again to verify that $2-\sqrt{1}$ and $-9-2\sqrt{17}$ are associates we have to show that one is unit times the other.

Now $-9-2\sqrt{17}=(2-\sqrt{17})\,(4+\sqrt{17})$ where $4+\sqrt{17}$ is a unit.

Also $2-\sqrt{17}=(-9-2\sqrt{17})\,(-4+\sqrt{17})$

where $-4+\sqrt{17}$ is a unit.

Hence $2-\sqrt{17}$ and $-9-2\sqrt{17}$ are associates.

§ 18 Characteristic of a ring.

Definition. *Consider the ring* $(R, +, .)$. $(R, +)$ *is the additive group of this ring each of whose element is of finite order* [*order of an element a of an additive group is the least +ive integer m such that* $m\,a=e$ *i.e. 0*].

Amongst the orders of the various elements of the group $(R, +)$ there will be a maximum integer say $n\ (> 0)$ then this n is said to be the characteristic of the ring $(R, +, .)$.

If however there exists no maximum for the orders of the elements of additive group $(R, +)$ then the ring is said to have characteristic zreo (or infinity).

Ex. 1. *Consider the ring* $(I_6, +_6, \times_6)$ *where*

$$I_6=\{0,1, 2, 3, 4, 5\}.$$

Let us consider the order of the various elements of additive group $(I_6, +_6)$ $o\ (0)=1$, $o\ (1)=6$, $o\ (2)=3$, $o\ (3)=2$. $o\ (4)=3$, $o\ (5)=6$.

The maximum order is 6 which we shall call as the characteristic of the above ring.

Ex. 2. *Consider the ring of integers* $(I, +, .)$.

Here the order of each element of the additive group $(I, +)$ except of the additive identity is of infinite order. Hence the ch. of the ring is zero.

Theorem 14. Ch. of a ring with unity.

The characteristic of a ring with unity is 0 *or* $n > 0$ *according as the unity element* 1 *(to be denoted by* e *for convenience sake) regarded as a member of the additive group of the ring has the order zero or* n.

Let us suppose that unity element e regarded as an element of additive group is of finite order say n so that

$$n\ e=0, \qquad \ldots(1)$$

Now consider any other element $a \in (R, +)$ then

$na=a+a+a+\ldots+n$ terms

$=e\ a+e\ a+e\ a+\ldots+e\ a$ $\qquad e\ a=1.a=a.$

$=(e+e+e+\ldots n$ terms$)\ a$ by Dist. Law

$=(n\ e)\ a=0\ (a)$ by $(1)=0$.

Hence order of any other element a is $\leqslant n$.

Therefore n is the maximum integer amongst the order of the various elements of the additive group $(R, +)$ of the ring which by definition is the characteristic of the ring with unity.

If the order of e be zero then that of ring will be zero.

As an exmple the ring $[I_6, +_6, \times_6]$ the unity element is 1 and its order is 6 when regarded as a member of the additive group as $6\,(1)=6=0$ the additive identity.

Hence order of this ring with unity is 6 as has been verified above in example 1.

Theorem 15. Ch. of an integral domain. (Lucknow 70)

The characteristic of an integral domain is 0 or $n > 0$ according as the order of any non zero element regarded as a member of the additive group of the integral domain is either zero or n.

Let I. D. be an integral domain *i.e.* a commutative ring with unity **without zero divisors** and a be any non zero element of it.

If this element is of zero order then the ch. of I. D. is also zero.

If the order of 'a' regarded as a member of additive group of I. D. is n then

$$n\,a=0. \qquad \ldots(1)$$

Again suppose b is any other non zero element of I. D. then $n\,a=0 \Rightarrow (n\,a)\,b=0.$

$\Rightarrow (a+a+a+\ldots n \text{ term})\,b=0$

$\Rightarrow (a\,b+a\,b+\ldots a\,b)=0$ by Dist. Law

$\Rightarrow a\,(b+b+b+\ldots n \text{ term})=0$ by Dist. Law

$\Rightarrow a\,(n\,b)=0$

But I. D. is without zero divisors and $a \neq 0$

$\therefore \quad a(nb)=0 \Rightarrow nb=0$

$\Rightarrow o(b) \leqslant n$ or $o(b) \leqslant o(a)$ ...(2)

Let $o(b)=m$ so that $mb=0$

$\therefore \quad 0=(mb)\,a=b\,(ma)$ as above

or $0=ma$ $\because$ $b\neq 0$ and D is without zero divisors

$\therefore \quad o(a) \leqslant m$ or $o(a) \leqslant o(b)$ ...(3)

From (2) and (3) it follows that $o(a)=o(b)$.

Hence every non zero element of I. D. is of the same finite order n so that the ch. of I. D. is also n

Theorem 16. *Every integral domain has a characteristic zero or prime.* **(Lucknow 70; Raj. M. Sc. 1966)**

Let I. D. be an integral domain and $a\neq 0$ be any element of it.

If order of a is zero then characteristic of D is zero. If order of a is finite say p *i.e.* $o(a)=p$ then the characteristic of D will also be p and we have to show that p is prime.

If p be not prime then p is composite $=p_1p_2$ where $p_1\neq 1$, $p_2\neq 1$ and $p_1 < p$, $p_2 < p$.

Now in an I.D. product of two non zero elements can not be zero as it is a ring without zero divisors.

$\therefore \quad a\neq 0 \Rightarrow a.a\neq 0 \Rightarrow a^2\neq 0$.

Also by Theorem 15 in an integral domain the order of any two non zero elements is same.

$\therefore \quad o(a)=p \Rightarrow o(a^2)=p \Rightarrow p\,a^2=0$

$\Rightarrow p_1\,p_2\,(a^2)=0 \Rightarrow (a^2+a^2+a^2+\ldots p_1p_2 \text{ times})=0$

$\Rightarrow (p_1\,a)\,(p_2\,a)=0$

$\Rightarrow$ either $p_1\,a=0$ or $p_2\,a=0$

as D is without zero divisors.

But $p_1\,a\neq 0$ as $p_1 < p$ and p is the least +ive integer s. t. $p\,a=0$ because $o(a)=p$. Similarly $p_2\,a\neq 0$. Hence a contradiction.

Therefore our supposition that p is composite is wrong and as such it should be prime only.

Theorem 17. *In an integral domain all non-zero elements generates additive cyclic group of the same order which is equal to the characteristic of the integral domain.*

(Allahabad 65, 68)

Ist Case. Characteristic of $D=0$

Let a be a non-zero element of D whose unity element is u say $\therefore \quad au=a=ua$

$$ma=m\,(au)=m\,(ua)=(mu)\,a \qquad \ldots(1)$$

Now $a\neq 0$ and if $m\neq 0$ then $ma\neq 0$ from I

Hence $ma=0$ only when $m=0$ showing thereby that the additive group generated by non-zero element a is of order zero.

2nd Case. Characteristic of $D=p$ where p is prime

$$pa=p\,(au)=p\,(ua)=(pu)\,a=0$$

Again $ma=0 \Rightarrow m=kp$. as $a\neq 0$, $m\neq 0$

Because $ma=m\,(ua)=(mu)\,a=0 \Rightarrow mu=0$

Hence p is least integer m s.t. $ma=0$

Therefore p is the order of addltive cyclic group generated by a.

Note. Characteristic of a field. **(Lucknow 70)**

Since every field is an integral domain therefore characteristic of a field F is 0 or $n>0$ according as the order of any non zero element (in particular the unity element regarded as a member of the addltive group) of F is zero or n

Working Rule. For characteristic of a ring with unity, integral domain or a field we should find the order of the unity element e regarded as a member of the additive group.

If the order of e is zero then ch. is zero and if it is finite say $n > 0$ then ch. is n.

Ex. 1. *Prove that the characteristic of field of Ex. 6. P. 174 is two.*

In this case zero of the ring is the element a

Also $a+a=a$, $b+b=a$, $c+c=a$, $d+d=a$

i.e. $2a=0$, $2b=0$, $2c=0$, $2d=0$ where 0 *i.e.* a is the additive identity.

Since order of each non zero element Is two and hence characteristic of this field is 2.

§ 19. Quotient field of an integral domain.

Definition.

A. Quotient in a field. *Let F be a field and $a, b \in F$ such that $b \neq 0$ then the unique solution of the equation $bx=a$ is called a quotient in F and is denoted by $\frac{a}{b}$.*

(Allahabad 68)

$b\,x=a \Rightarrow b^{-1}\,bx=b^{-1}\,a \Rightarrow 1.x=b^{-1}\,a \Rightarrow x=b^{-1}\,a$.

Since field is commutative $b^{-1}\,a=a\,b^{-1}$

$\therefore \quad x=b^{-1}\,a=a\,b^{-1}$ and is denoted by $\frac{a}{b}$, where $b \neq 0$.

B. Equality, Addition and Multiplication of quotients in F.

Let $\frac{a}{b}$ and $\frac{c}{d}$ be any two quotients in F such that $b \neq 0, d \neq 0$.

Equality. $\frac{a}{b}=\frac{c}{d} \Leftrightarrow a\,d=b\,c$.

$$\frac{a}{b}=\frac{c}{d} \Rightarrow a\,b^{-1}=c\,d^{-1} \Rightarrow b^{-1}\,a=c\,d^{-1}$$

$$\Rightarrow b\,b^{-1}\,a=b\,c\,d^{-1} \Rightarrow a=b\,c\,d^{-1}$$

$$\Rightarrow a\,d=b\,c\,d^{-1}d \Rightarrow a\,d=b\,c.$$

Conversely let $a\,d=b\,c \Rightarrow a\,d\,d^{-1}=b\,c\,d^{-1}$

$$\Rightarrow b^{-1}\,a\,d\,d^{-1}=b^{-1}\,b\,c\,d^{-1}$$

$$\Rightarrow b^{-1}\,a=c\,d^{-1} \Rightarrow a\,b^{-1}=c\,d^{-1}$$

$$\Rightarrow \frac{a}{b}=\frac{c}{d}.$$

Addition $\dfrac{a}{b}+\dfrac{c}{d}=\dfrac{a\,d+b\,c}{b\,d}$

$$\frac{a}{b}+\frac{c}{d}=a\,b^{-1}+c\,d^{-1}=b^{-1}\,a+c\,d^{-1}$$

$$=b^{-1}\,a\,d\,d^{-1}+b^{-1}\,b\,c\,d^{-1}$$

$\because\quad d\,d^{-1}=1,\ b^{-1}\,b=1$ in a field

$$=(b^{-1}\,a\,d+b^{-1}\,b\,c)\,d^{-1}$$

distributive property in a field.

$$=b^{-1}\,(a\,d+b\,c)\,d^{-1}=\frac{a\,d+b\,c}{b\,d}.$$

Multiplication.

$$\frac{a}{b}\cdot\frac{c}{d}=(a\,b^{-1})\,(c\,d^{-1})=a\,(b^{-1}\,c)\,d^{-1}$$

$$=a\,(c\,b^{-1})\,d^{-1} \quad \because\ b^{-1}\,c=c\,b^{-1}$$

$$=(a\,c)\,(b^{-1}\,d^{-1})=(a\,c)\,(d\,b)^{-1}$$

$$=\frac{a\,c}{d\,b}=\frac{a\,c}{b\,d} \qquad \because\quad d\,b=b\,d \text{ in a field.}$$

C. Equivalence relation.

Consider the set $S=D\times D_0$ where D is an integral domain *i.e.* commutative ring without zero divisors and with unity and D_0 is the set of non zero elements of D.

$\therefore$ S is the set of ordered pairs $(a, b) : a \in D, b \in D_0$.

Let us define a binary relation $\sim$ in S given by

$(a, b) \sim (c, d)$ if $a\,d=b\,c$.

The above relation is an equivalence relation in S.

Reflexive. $(a, b) \sim (a, b) \quad \because \quad a\,b=b\,a$

by commutative property in D.

Symmetric. $(a, b) \sim (c, d) \Rightarrow a\,d=b\,c$

$\Rightarrow c\,b=d\,a \Rightarrow (c, d) \sim (a, b)$.

Transitive. $(a, b) \sim (c, d)$ *i.e.* $a\,d=b\,c$

$(c, d) \sim (e, f)$ *i.e.* $c\,f=d\,e$

To prove $(a, b) \sim (e, f)$ or $a\,f=b\,e$.

Now $a\,d=b\,c \Rightarrow a\,d\,f=b\,c\,f$

and $c\,f=d\,e \Rightarrow b\,c\,f=b\,d\,e$.

$\therefore \quad a\,d\,f=b\,d\,e$ or $a\,(d\,f)=b\,(d\,e)$

or $a\,f\,d=b\,e\,d \Rightarrow (a\,f-b\,e)\,d=0$

Now the integral domain D is without zero divisors and $d\neq 0$.

$\therefore \quad (a\,f-b\,e)\,d=0 \Rightarrow a\,f-b\,e=0 \Rightarrow a\,f=b\,e$

$\Rightarrow (a, b) \sim (e, f)$. Hence transitive.

Hence the relation $\sim$ in the set $S=D\times D_0$ is an equivalence relation so that it partitions the set P into mutually disjoint equivalence classes.

We shall denote by $\frac{a}{b}$ the set of all ordered pairs (x, y) of $D\times D_0$ which are such that $(x, y) \sim (a, b)$.

$\therefore \quad \frac{a}{b}=\{(x, y) : (x, y) \sim (a, b)\}$.

These equivalence classes are our quotients.

D. Definition of addition and multiplication of equivalence classes.

$$\frac{a}{b}+\frac{c}{d}=\frac{a\,d+b\,c}{b\,d}.$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{a\,c}{b\,d}$$ where $b\,d\neq 0$ as $b\neq 0$, $d\neq 0 \Rightarrow b\,d\neq 0$ as D is a ring without zero divisors.

E. Set K of all equivalence classes is a field with respect to operations of addition and multiplication defined in part D.

$$K=\left\{\frac{a}{b} : \frac{a}{b}, \text{ is an equivalence class}\right\}$$

We have to verify the postulates of a field for K.

I. The set (K, +) is an additive abelian group.

Addition is Associative.

$$\left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}=\frac{a\,d+b\,c}{b\,d}+\frac{e}{f}=\frac{(a\,b+b\,c)\,f+b\,d\,e}{b\,d\,f}$$

$$=\frac{a\,d\,f+b\,c\,f+b\,d\,e}{b\,d\,f}=\frac{a\,d\,f+b\,(c\,f+d\,e)}{b\,d\,f}$$

$$\frac{a}{b}+\frac{c\,f+d\,e}{a\,f}=\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right)$$

Additive identity.

$$\frac{a}{b}+\frac{0}{d}=\frac{a\,d+b.0}{b\,d}=\frac{a\,d}{b\,d}=\frac{a}{b}$$

Hence $\frac{0}{d}$ is the additive identity. We can also say that $\frac{0}{1}$ is the additive identity as $\frac{0}{d}$ and $\frac{0}{1}$ are the same equivalence class.

Additive Inverse.

$$\frac{a}{b}+\frac{-a}{b}=\frac{a\,b+b\,(-a)}{b^2}=\frac{a\,b-a\,b}{b^2}=\frac{0}{b^2}=\frac{0}{1}$$

$$\because \quad 1.0=b^2.0$$

Hence $-\frac{a}{b}$ is the additive inverse of $\frac{a}{b}$.

Addition is commutative.

$$\frac{a}{b}+\frac{c}{d}=\frac{a\,d+b\,c}{b\,d}=\frac{c\,b+d\,a}{d\,b}=\frac{c}{d}+\frac{a}{b}.$$

2. Multiplication is associative.

$$\left(\frac{a}{b}\cdot\frac{c}{d}\right)\cdot\frac{e}{f}=\frac{a\,c}{b\,d}\cdot\frac{e}{f}=\frac{a\,(c\,e)}{b\,(d\,f)}=\frac{a}{b}\left(\frac{c}{d}\cdot\frac{e}{f}\right).$$

Multiplication distributes addition.

$$\frac{a}{b}\left(\frac{c}{d}+\frac{e}{f}\right)=\frac{a}{b}\cdot\frac{cf+de}{df}=\frac{a(cf+de)}{bdf}=\frac{ba(cf+de)}{b^2df}$$

$$=\frac{(ac)(bf)+(bd)(ae)}{(bd)(bf)}=\frac{ac}{bd}+\frac{ae}{bf}$$

$$=\frac{a}{b}\cdot\frac{c}{d}+\frac{a}{b}\cdot\frac{e}{f}.$$

Similarly we can prove the orther distributive law.

Multiplicative Identity.

$$\frac{a}{b}\cdot\frac{1}{1}=\frac{a\cdot 1}{b\cdot 1}\equiv\frac{a}{b}$$

$\therefore$ $\frac{1}{1}$ is the multiplicative identity,

In general any equivalence $\frac{x}{x}$ with $x\neq 0$ is the multiplicative identity.

Multiplicative inverse of non zero elements.

Let $\frac{a}{b}, b\neq 0 \in K$ and since $\frac{a}{b}\neq 0 \quad \therefore \quad a\neq 0$

Also $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)\equiv\frac{ab}{ba}=\frac{ab}{ab}=\frac{1}{1}$.

Hence $\frac{b}{a}$ such that $a\neq 0$ is the multiplicative inverse of $\frac{a}{b}$.

Hence K is *a* commutative ring with unity such that every non zero element is inversible and hence K is a field.

Quotient field of D.

The above field is called field of quotients of D.

F. The field of quotient k of D contains an integral domain D′ which is isomorphic to D

Let $D'=\left\{\frac{a}{1} : a \in D\right\}$

cosider the mapping $f: D \to D'$ defined as

$$f(a) = \frac{a}{1} . \in D'$$

we shall establish that f is an isomorphism.

f is one-one. $f(a) = f(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a \cdot 1 = b \cdot 1$

$$\Rightarrow a = b$$

f is onto. If $\frac{a}{1} \in D'$ then $a \in D$ whose f image is

$$\frac{a}{1}.$$

f preserves the two compositions.

$$f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$$

$$f(ab) = \frac{ab}{1} = \left(\frac{a}{1}\right)\left(\frac{b}{1}\right) = f(a)\, f(b)$$

Hence $f: D \to D'$ is an isomorphism

$$\therefore \quad D \cong D'$$

G. The field of quotients k of I. D. D. is smallest field containing D′ which is the isomorphic copy of D

Let K' be another field containing D'

then $\frac{a}{1}, \frac{b}{1} \in K' \ \forall \ a, b \in D.$

Choose $\frac{a}{b} \in K$ such that $b \neq 0$.

Now $\frac{b}{1}$ with $b \neq 0$ is non zero element of K' so that its inverse $\left(\frac{b}{1}\right)^{-1} = \frac{1}{b}$ also belongs to K'

Now $\frac{a}{1}, \frac{1}{b} \in K' \Rightarrow \left(\frac{a}{1}\right)\left(\frac{1}{b}\right) = \frac{a}{b} \in K'$

$$\therefore \quad \frac{a}{b} \in K \Rightarrow \frac{a}{b} \in K'$$

$$\therefore \quad K \subseteq K'$$

Hence K is the smallest field which contains an isomorphic copy D' of integral domain D.

The result C, D, E, F proved above lead to the proof of the following theorem.

A commutative ring without zero divisors can be imbeded in a field.

or

Every integral domain can be imbeded in a field.

(Utkal 70; Benares 70; Agra M. Sc. 69; Raj. M. Sc. 69)

or

It is possible to construct a field (quotient field) from the elements of an integral domain D which contains a sub set D' isomorphic to D. **(Delhi 69)**

Give the proofs of C, D, E

Theorem 18 (A). *Any field F containing an integral domain D contains a sub field isomorphic to the quotient filed K of D. In other words the quotient field of an integral domain D is the minimum extension of D to a field.*

(Benares M. Sc. 69, 70)

Now D is contained in F and let $a \in D$ and $b \neq 0 \in D$ and hence $a \in F$ and $b \neq 0 \in F \Rightarrow ab^{-1} \in F$

Choose F' to be the sub set of F whose elements are of the form ab^{-1} where $a \in D$, $b \neq 0 \in D$.

We will first show that F' forms a sub field. The criteria for which are

(i) $a \in F', b \in F' \Rightarrow a-b \in F'$

(ii) $a \in F', b \neq 0 \in F' \Rightarrow ab^{-1} \in F'$ § 14 P. 223

Let ab^{-1}, cd^{-1} ($b\neq0$ and $d\neq0$) $\in F'$

then $ab^{-1}-cd^{-1}=a\,d\,d^{-1}\,b^{-1}-c\,b\,b^{-1}\,d^{-1}$

$=ad\,d^{-1}\,b^{-1}-bc\,d^{-1}\,b^{-1}$

$=(ad-bc)\,d^{-1}\,b^{-1}$

$=(ad-bc)\,(bd)^{-1}\in F'$

as $ad-bc\in F$ and $bd\neq0\in D$

Above proves the first criteria. For the 2nd criteria we have $ab^{-1}, cd^{-1}\in F'$ $b\neq0$, $d\neq0$

Suppose $cd^{-1}\neq0\Rightarrow c\neq0$

Now $(ab^{-1})\,(cd^{-1})^{-1}=(ab^{-1})\,(dc^{-1})=ad\,(cb)^{-1}\in F'$ because $ad\in D$ and $c\neq0$, $b\neq0$, $cb\neq0\in D$ and D is contained in F,

$\therefore$ $(ad)\,(cb)^{-1}\in F$ and hence $\in F'$ by definition of F'.

Hence F' is a sub field of F

2nd Part. Now we shall establish that the quotient field K is isomorphic to F'.

$$K=\left\{\frac{a}{b}:a\in D,\ l\neq0\in D\right\}$$

$$F'=\{ab^{-1}:a\in D,\ b\neq0\in D\}$$

Consider a mapping $f: K\to F'$ defined as

$$f\left(\frac{a}{b}\right)=ab^{-1}\ \forall\ a/b\in K \text{ and } ab^{-1}\in F'$$

f is one-one :

$$f\left(\frac{a}{b}\right)=f\left(\frac{c}{d}\right)\Rightarrow ab^{-1}=cd^{-1}$$

$$\Rightarrow ab^{-1}\,bd=cd^{-1}\,bd$$

$$\Rightarrow ad=cb\,d^{-1}d$$

$$\Rightarrow ad=bc$$

$$\Rightarrow (a,b)\sim(c,d)$$

$$\Rightarrow \frac{a}{b}=\frac{c}{d}\ \therefore\ f \text{ is one-one}$$

Again f is onto obviously.

In order to prove f to be an isomorphism we have only to establish that f preserves the compositions

$$f\left(\frac{a}{b}+\frac{c}{d}\right)=f\left(\frac{ad+bc}{bd}\right)=(ad+bc)\ (bd)^{-1}$$
$$=(ad+bc)\ (d^{-1}\ b^{-1})$$
$$=ad\ d^{-1}\ b^{-1}+bc\ d^{-1}\ b^{-1}$$
$$=ab^{-1}+bc\ d^{-1}\ b^{-1}$$
$$=ab^{-1}+cd^{-1}$$
$$=f\left(\frac{a}{b}\right)+f\left(\frac{c}{d}\right)$$

$$f\left(\frac{a}{b}\cdot\frac{c}{d}\right)=f\left(\frac{ac}{bd}\right)=(ac)\ (bd)^{-1}$$
$$=(ac)\ (d^{-1}\ b^{-1})$$
$$=(ab^{-1})\ (cd^{-1})=f\left(\frac{a}{b}\right)f\left(\frac{c}{d}\right)$$

Hence $f : K \to F'$ is an isomorphism.

$\therefore \quad K \cong F' \quad$ or $\quad F' \cong K$

Theorem 18. (B) *Any two isomorphic integral domains D_1 and D_2 have isomorphic quotient fields.* **(Benares M. Sc. 65)**

Since $D_1 \cong D_2$ $\exists$ *a* mapping $f : D_1 \to D_2$ such that f is one-one-onto and preserves the compositions.
so that $f(a+b)=f(a)+f(b)$ and $f(ab)=f(a).\ f(b)$.

where $a, b \in D_1$ and $f(a), f(b) \in D_2$.

Choose $F_1=\left\{\frac{a}{b} : a, b \in D_1, b\neq 0\right\}$

$$F_2=\left\{\frac{f(a)}{f(b)} : f(a), f(b) \in D_2, f(b)\neq 0\right\}$$

be the quotient fields of integral domains D_1 and D_2
we have to prove that $F_1 \cong F_2$.

Consider the mapping $\phi : F_1 \to F_2$ defined as

$$\phi\left(\frac{a}{b}\right)=\frac{f(a)}{f(b)} \qquad \forall \frac{a}{b} \in F_1$$

ϕ is one-one. $\phi\left(\frac{a}{b}\right)=\phi\left(\frac{c}{d}\right) \Rightarrow \frac{f(a)}{f(b)}=\frac{f(c)}{f(d)}$

$\Rightarrow f(a)\, f(d)=f(b)\, f(c)$

$\Rightarrow f(a\, d)=f(b\, c)$

$\Rightarrow ad=bc$ as f is one-one

$\Rightarrow \frac{a}{b}=\frac{c}{d}$.

ϕ is onto. Corresponding to each element $\frac{f(a)}{f(b)} \in F_2$ $\exists$ an element $\frac{a}{b} \in F_1$ such that $\phi\left(\frac{a}{b}\right)=\frac{f(a)}{f(b)}$.

ϕ preserves the compositions.

$$\phi\left(\frac{a}{b}+\frac{c}{d}\right)=\phi\left(\frac{ad+bc}{bd}\right)=\frac{f(ad+bc)}{f(bd)}$$

$$=\frac{f(ad)+f(bc)}{f(b)\, f(d)}=\frac{f(a)\, f(d)+f(b)\, f(c)}{f(b)\, f(d)}$$

$$=\frac{f(a)}{f(b)}+\frac{f(c)}{f(d)}=\phi\left(\frac{a}{b}\right)+\phi\left(\frac{c}{d}\right)$$

$$\phi\left(\frac{a}{b}\cdot\frac{c}{d}\right)=\phi\left(\frac{ac}{bd}\right)=\frac{f(ac)}{f(bd)}=\frac{f(a)\, f(c)}{f(b)\, f(d)}$$

$$=\frac{f(a)}{f(b)}\cdot\frac{f(c)}{f(d)}=\phi\left(\frac{a}{b}\right)\cdot\phi\left(\frac{c}{d}\right)$$

Hence $\phi : F_1 \to F_2$ is a one-one-onto mapping which preserves the two compositions. Therefore $F_1 \cong F_2$

§ 20. Ideals

Definition.

(a) **Left Ideal.** $(R, +, .)$ is a ring and S is any non empty sub set of R. Then S is said to be *a* left ideal of R if

(i) *S is a sub group of R w. r. t.* **addition**

i.e. $\forall\ a, b \in S \quad a-b \in S.$

(ii) $r\,s \in S \quad \forall\ r \in R$ *and* $\forall\ s \in S$. [*r on the left*]

(b) **Right ideal.** for right ideal the condition (ii) will change as under

$s\,r \in S \quad \forall\ r \in R$ *and* $\forall\ s \in S$. [*r on the right*]

(Kanpur M. Sc. 70, 71; Kurkshetre 70; Lucknow 69; Benares 61, 70)

(c) **Ideal.** (Two sided ideal).

For ideal the condition (ii) will change as under.

$r\,s \in S$ *and* $s\,r \in S \quad \forall\ r \in R$ *and* $\forall\ s \in S.$

i.e. S is both left as well as right ideal of R.

(Lucknow 68, 70)

(d) **Every ideal S of a ring R is a sub ring of R**

We know the criteria for a sub ring is

(i) $\forall\ a, b \in S \quad a-b \in S$

i.e. S is *a* sub group of $(R, +)$.

(ii) $\forall\ a, b \in S \quad a\,b \in S$ *i.e.* closure property.

Now if S is an ideal then by condition (i) we get the condition (1) for sub ring.

Also condition (ii) of ideal gives

$$r\,s \in S, \quad s\,r \in S \quad \forall\ r \in R, \forall\ s \in S.$$

It can be written as $r\,s \in S, s\,r \in S \quad \forall\ r \in S,$

$\forall\ s \in S.$

$\because \quad S \subseteq R \quad \therefore \quad r \in S \Rightarrow r \in R.$

Hence condition (ii) for ring *i.e.* closure property is satisfied.

Therefore every ideal S of *a* ring R is *a* sub ring of R

(e) **Every sub ring S of a ring R is not an ideal.**

This is true because the condition (ii) of sub ring will

not give us condition (ii) for an ideal as in part *d*, for sub ring we are given

$$r\,s \in S, \quad \forall\ r \in S, \quad \forall\ s \in S$$

This will not lead to

$$r\,s \in S\ \forall\ r \in R, \ \forall\ s \in S$$

because $r \in R$ does not imply that $r \in S$, as this r may be or may not be in S

(f) Ideal of a commutative ring

If r is *a* commutative ring then

$$a\,b = b\,a\ \forall\ a, b \in R.$$

or $r\,s = s\,r\ \forall\ r, s \in R$. given

or $r\,s = s\,r\ \forall\ r \in R$ and $\forall\ s \in S$.

as $s \in S \Rightarrow s \in R$.

Therefore every left ideal is also a right ideal and hence it is an ideal. Hence the condition (ii) for ideal in a commutative ring can be stated as

$$r\,s \in S\ \forall\ r \in R \text{ and } \forall\ s \in S.$$

(g) Proper and improper ideals.

Every ring R has two improper ideals one of which is R itself called the **unit ideal** the other being the singleton $\{0\}$ known as **zero or null ideal.** Any other ideal of R except these two is called proper ideal. If a ring has no proper ideal then it is called a **simple ring.**

Exercise 6

1. *Consider the sets* S_1, S_2, S_3, S_4 *of matrices of the form*

(i) $\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ (ii) $\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}$ (iii) $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ (iv) $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$

(Meerut 1970)

with a, b as integers, and R is ring of all 2×2 *matrices whose elements are integers then prove the following.*

(i) S_1 *and* S_4 *are right ideals but not the left.*

(*ii*) *S_2 is left ideal but not the right.*

(*iii*) *S_3 is neither a left nor a right ideal.*

The condition I for an ideal is clearly satisfied in all the three sets.

i.e. $A, B \in S_1, S_2, S_3 \Rightarrow A-B. \in S_1, S_2, S_3$

i e. S_1, S_2, S_3 are sub groups of $(R,+)$

The condition (ii) is

$s_1 r \in S_1 \ \forall\ r \in R$ and $\forall\ s_1 \in S_1$ for right ideal

$r s_2 \in S_2 \ \forall\ r \in R$ and $s_2 \in S_2$ for left ideal.

Choose $s_1=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ and $r=\begin{bmatrix} c & d \\ e & f \end{bmatrix}$

$$\therefore \quad s_1 r=\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}\begin{bmatrix} c & d \\ e & f \end{bmatrix}=\begin{bmatrix} ac+be & ad+bf \\ 0 & 0 \end{bmatrix} \in S_1$$

$\therefore$ S_1 is a right ideal.

Also $r s_1=\begin{bmatrix} c & d \\ e & f \end{bmatrix}\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} ca & cb \\ ea & eb \end{bmatrix} \notin S_1$

$\therefore$ S_1 is not a left ideal.

Similarly we can prove that S_2 is left ideal but not *a* right ideal

Now $s_3=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \in S_3$ and $r=\begin{bmatrix} c & d \\ e & f \end{bmatrix}$.

then $s_3\ r=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}\begin{bmatrix} c & d \\ e & f \end{bmatrix}=\begin{bmatrix} a\,c & a\,d \\ b\,e & b\,f \end{bmatrix} \notin S_3$.

and $r\ s_3=\begin{bmatrix} c & d \\ e & f \end{bmatrix}\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}=\begin{bmatrix} c\,a & d\,b \\ e\,a & f\,b \end{bmatrix} \notin S_3$

Hence S_3 is neither *a* left nor *a* right ideal.

2. *The sub set I of integers is only a sub ring but not an ideal of the ring of rational numbers* $(Q, +, .)$.

We know that product and difference of two integers is again an integer. *i.e.* $\forall\ a, b \in I$ we have $a-b \in I$ and $a\,b \in I$. and hence by Th. P. 218 is *a* sub ring.

For ideal. The product of an integer and *a* rational number is not an integer

i.e. $r\,s. \notin I \;\forall\; r \in Q$ and $s \in I$.

$r=\frac{1}{2}$, $s=3$ but $\frac{1}{2}\cdot 3$ is not an integer and as such $\notin I$

Similarly the set Q of rational numbers is only sub ring but not an ideal of the ring of real numbers $(R, +, .)$
as $r=\sqrt{5} \in R$, $s=\frac{1}{2} \in Q$ then $r\,s=\sqrt{5}/2 \notin Q$.

3. *Prove that the set* $S=\{x\,m : x$ *is an integer*$\}$ *and* m *is a fixed integer in an ideal of the ring* R *of all integers.*

Let $x_1\,m, x_2\,m \in S$ where x_1, x_2 are integers so that x_1-x_2 is also an integer

then $x_1\,m-x_2\,m=(x_1-x_2)\,m \in S$

Again let r be any integer then

$r\,s_1=r\,(x\,m)=(r\,x)\,m \in S$ as $r\,x$ is again an integer and hence S is a left ideal. Now since the ring of integers is a commutative ring and as such left ideal is also a right ideal therefore S is an ideal.

4. *If* R *is a ring and* $a \in R$ *and let*

$$S=\{x \in R : a\,x=0\}$$

prove that S *is a right ideal of* R.

Let $x_1, x_2 \in S$ so that $a\,x_1=0$, $a x_2=0$
and hence $ax_1-ax_2=0$

or $\quad a\,(x_1-x_2)=0 \Rightarrow x_1-x_2 \in S.$

$\therefore$ Condition (i) of an ideal is satisfied.

Let $r \in R$. and $x \in S$ *i.e.* $ax=0$
then $x\,r$ should be shown to belong to S if S is a right ideal.

Consider $a\,(x\,r)=(a\,x)\,r=0.r=0$
Since $a\,(x\,r)=0 \Rightarrow x\,r \in S$
$\therefore$ S is a right ideal

§ 21. Certain Theorems

Theorem 19. (A) *Prove that the intersection of two ideals of a ring R is an ideal of R* **(Kurkshetra 69)**

Let S and T be two ideals of ring R so that both of them are sub groups of R and hence their intersection $S \cap T$ is also *a* sub group of R under addition. Therefore the condition (i) for an ideal is satisfied.

Now cloose any $s \in S \cap T \Rightarrow s \in S$ and $s \in T$.

S is an ideal $\Rightarrow r\,s \in S, s\,r \in S$

$\forall\ r \in R$, and $\forall\ s \in S$.

T is an ideal $\Rightarrow r\,s \in T, s\,r \in T$

$\forall\ r \in R$ and $\forall\ s \in T$.

From above we conclude that

$s\,r \in S, s\,r \in T \Rightarrow s\,r \in S \cap T$.

and $r\,s \in S, r\,s \in T \Rightarrow r\,s \in S \cap T$

$\therefore\ \forall\ s \in S \cap T$ and $\forall\ r \in R$ we have

$r\,s \in S \cap T$ and $s\,r \in S \cap T$.

Hence $S \cap T$ is both left and right ideal and as such it is an ideal.

Theorem 19. (B) *Prove that the intersection of an arbitrary family of ideals of a ring is itself an ideal.* **(Benares 61)**

Let A be an arbitrary family of ideals of *a* ring $(R, +, .)$ Choose $S^* = \cap\{S : S \in A\}$

We have to show that S^* is an ideal for which we shall use the criteria laid down in (C) Page. 246

Let $a \in S^*$ and $r \in R$, then by definition of intersection $a \in S$ for all $S \in A$

Again each S is an ideal we have by definition $a \in S$, $r \in R \Rightarrow a\,r \in S,\ r\,a \in S\ \forall\ S \in A$

$\Rightarrow a\,r \in S^*$ and $r\,a \in S^*$

Hence S^* is an ideal

In a similar manner we can prove the intersection of an

arbitrary family of left ideals of a ring is a left ideal.

(Benares M.Sc. 66)

Tbeorem 20. *A field F has no proper ideals. In other words the only ideals of a field are* {0} *and F itself.*

(Delki 70; B.H.U. 70 Kanpur M.Sc. Stat 71; Meerut M.Sc. 67)

Let S be an ideal of field F then we will prove that either $S=\{0\}$ or $S=F$.

In case S be a non zero ideal and a be any non zero element of S

then a^{-1} will exist and shall belong to field F.

Now $a \in S$ and $a^{-1} \in F \Rightarrow a\,a^{-1} \in S$ as S is an ideal

or $1 \in S$.

Now $1 \in S$ and let $x \in F \Rightarrow 1\,x \in S \Rightarrow x \in S$.

Thus every element $x \in F$ is also an element of ideal S.

$\therefore$ $F \subseteq S$ but $S \subseteq F$ and hence $S=F$

Hence the only ideals of a field are {0} and F itself.

Theorem 21 (A) *If R is a commutative ring and* $a \in R$ *then*

$Ra=\{ra : r \in R\}$ *in an ideal of R.*

(B) *A non zero commutative ring with unity is a field if it has no proper ideals.* **(Benares 61; Kanpur 71; Meerut M.Sc. 67, 69; Rajasthan M.Sc. 06, 67)**

(A) Let $p, q \in Ra \Rightarrow p=r_1a, q=r_2a$ where $r_1, r_2 \in R$.

$\therefore$ $p-q=r_1a-r_2a=(r_1-r_2)\,a=r\,a \in Ra$

where $r=r_1-r_2 \in R$.

$\therefore$ $p, q \in Ra \Rightarrow p-q \in Ra$ and hence condition (i) of an ideal is satisfied.

Again let $x \in R$ and $p \in Ra$ so that $p=r_1\,a$.

then $x\,p=x\,(r_1a)=(xr_1)\,a \in Ra$ as $x\,r_1 \in R$.

Therefore $R\,a$ is a left ideal and since the ring is commutative it as also right ideal or simply an ideal.

(B) Given R is a commutative ring with unity with no proper ideals which in other words means that its only ideals are $\{0\}$ and R itself. In order to prove that it is a field we must establish the third property of field *i.e.* every non zero element has a multiplicative inverse.

Choose $a \neq 0$ to be any element of R, then the set

$R\,a = \{r\,a : r \in R\}$, is an ideal of R as shown in A

Now R is with unity therefore $1 \in R$ and as such $1.a = a \in R\,a$. Hence $a \neq 0 \in R\,a$ and therefore this ideal Ra is not zero ideal. Further it is given that R has no proper ideals *i.e.* its only ideals could be either $\{0\}$ or R itself. Since ideal $R\,a$ is not $\{0\}$ therefore it follows that $Ra = R$ *i.e.* every element of R is a multiple of a by some element of R.

Now $1 \in R$ and by virtue of the fact that $R = Ra$ we must have an element $b \in R$ so that $1 = ba \Rightarrow a^{-1} = b$.

Thus every non zero element has an inverse.

$\therefore$ R is a field.

Theorem 22. *If an ideal S of a ring R contains a unit of R then $S = R$.*

Recall the definition of units as given in § 17. P. 228. R is a ring with unity 1 and a be a unit element of R then by definition a^{-1} exists and belongs to R.

Now by definition unit $a \in$ ideal S

also $a^{-1} \in$ Ring R

Hence $a\,a^{-1} \in S$ or $1 \in S$ by def. of ideal

we have to prove that $S = R$

Let x be any element of R then $x \in R$; $1 \in S$

$$\Rightarrow x.1 \in S$$
$$\Rightarrow x \in S$$
$$\therefore \quad R \subseteq S$$

Also $S \subseteq R$ as S is an ideal of R

Hence from above we get $R=S$

§ 22. Smallest left ideal containing a given sub set S.

Def. *If M be a given non empty sub set of a ring R, then a left ideal I of R is called the smallest left ideal of R containing M if*

(*a*) *I contains M or M is contained in I i.e. $M \subseteq I$.*

(*b*) *I is contained in every left ideal of R containing M.*

Left ideal generated by M.

This smallest left ideal of R containing M will be termed as the left ideal generated by M and denoted as (M).

Similarly we can define the right ideals generated by M or ideals generated by M.

Exercise 7

1. *The left ideal generated by the union $I_1 \cup I_2$ of two left ideals is the set I_1+I_2 consisting of the elements of R obtained by adding any element of I_1 to any element of I_2.*

(Meerut B. Sc. Summer 1970)

Here $S = I_1 \cup I_2$ where I_1, I_2 are two left ideals

we have to prove that I_1+I_2 is ideal generated by $I_1 \cup I_2$, For this we will first establish that

(1) I_1+I_2 is a left ideal.

(2) $I_1+I_2 \subseteq I_1 \cup I_2$

(3) If any left ideal contains $I_1 \cup I_2$ then I_1+I_2 is also contained in it.

Proof. **I_1+I_2 is a left ideal.**

Let $p=a_1+a_2$, $q=b_1+b_2 \in I_1+I_2$

so that $a_1, b_1 \in I$, $a_2, b_2 \in I_2$

or $a_1-b_1 \in I_1$, $a_2-b_2 \in I_2$ as I_1 and I_2 are ideals ...(1)

Now $p-q=(a_1+a_2)-(b_1+b_2)=(a_1-b_1)$

$+(a_2-b_2) \in I_1+I_2$ by (1)

Thus I_1+I_2 is a sub group of R and first condition of being a left ideal is satisfied.

In order to verify the second property for an ideal.

Choose $r \in R$ and $p=a_1+a_2 \in I_1+I_2$.

then $r\,p$ should belong to I_1+I_2

$\forall\ r \in R$ and $\forall\ p \in I_1+I_2$

$r\,p=r\,(a_1+a_2)=r\,a_1+r\,a_2 \in I_1+I_2$

because $r\,a_1 \in I_1$ as I_1 is a left ideal

$r\,a_2 \in I_2$ as I_2 is a left ideal.

Thus the second property is also satisfied.

Hence I_1+I_2 is a left ideal of R.

Now $a_1 \in I_1.\ 0 \in I_2 \quad \therefore \quad a_1+0 \in I_1+I_2$

$\therefore \quad I_1 \subseteq I_1+I_2$

Again $0 \in I_1,\ a_2 \in I_2 \quad \therefore \quad 0+a_2 \in I_1+I_2$

$\therefore \quad I_2 \subseteq I_1+I_2$

Hence $I_1 \cup I_2 \subseteq I_1+I_2$.

Thus the left Ideal I_1+I_2 contains $I_1 \cup I_2$.

Again if any left ideal contains $I_1 \cup I_2$ then it must contain I_1+I_2.

Thus I_1+I_2 is the left ideal which is contained in every left ideal containing $I_1 \cup I_2$

Hence I_1+I_2 is smallest left ideal containing $I_1 \cup I_2$ and by definition it is the left ideal generated by $I_1 \cup I_2$

2. *Prove that S is an ideal of $S+T$ where S is any ideal of a ring R and T is any sub ring of R.* **(Meerut 69)**

Here we shall prove that $S+T$ is a sub ring then establish that $S \subseteq S+T$ where S is an ideal of R and hence S will be an ideal of $S+T$.

S+T is a sub ring.

$p=a+\alpha$, $q=b+\beta$, $\in S+T$ where

$a, b \in S$; $\alpha, \beta \in T$

$\Rightarrow ab \in S$ as S being an ideal is also a sub ring.

Also $\alpha\beta \in T$ as T is a sub ring.

Agian S is an ideal

$\therefore \quad a \in S, \beta \in T$ *i.e.* $\beta \in R \Rightarrow a\beta \in S$

$b \in S, \alpha \in T$ *i e.* $\alpha \in R \Rightarrow \alpha b \in S$

Now $pq=(a+\alpha)\ (b+\beta)=(ab+\alpha b+a\beta)+\alpha\beta$

As discussed each of the element in the first bracket $\in S$ and in theond itb els cengs to T

$\therefore \quad pq \in S+T \ \forall\ p, q \in S+T$.

Also $p-a=(a+\gamma)-(b+\beta)=(a-b)+(\gamma-\beta) \in S+T$

as $a-b \in S$ which is a sub ring or ideal, $\gamma-\beta \in T$ when R is a sub ring.

Therefore $S+T$ is a sub ring of R.

Again $a \in S, 0 \in T \qquad \therefore \qquad a+0 \in S+T$

Hence $S \subset S+T$.

Now S being an ideal of R, $S \subset S+T$ and $S+T$ being a sub ring, all these imply that S is also an ideal of $S+T$

3. *If I_1, I_2 are two ideals of a ring then the set S of all elements of R of the form $a_1 a_2+b_1 b_2+c_1 c_2+ \ldots +l_1 l_2$ where $a_1, b_1, \ldots, l_1 \in I_1$ and $a_2, b_2, \ldots, l_2 \in I_2$ is an ideal of R.*

(Meerut 70; Lucknow 70)

Let $p=a_1a_2+b_1b_2+ \ldots +l_1l_2 \in S$

$q=p_1p_2+q_1q_2+ \ldots +y_1y_2 \in S$

then $p-q=(a_1a_2+b_1b_2+ \ldots +l_1l_2)-(p_1p_2+q_1q_2+ \ldots +y_1y_2)$.

$=(a_1a_2+b_1b_2+ \ldots +l_1l_2)+(-p_1)\ p_2$

$+(-q_1)\ q_2+ \ldots +(-y_1)\ y_2$

Now $p_1 \in I_1$ which is an ideal $\Rightarrow -p_1 \in I_1$, $p_2 \in I_2$

Hence $p-q$=an element of S+an element of S=element of S.

Now choose $r \in R$ and $p=\Sigma a_1 a_2 \in S$. Then

$rp=r\,(a_1a_2+b_1b_2+\ldots+l_1l_2)$

$=(r\,a_1)\,a_2+(r\,b_1)\,b_2+\ldots\ldots+(r\,l_1)\,l_2$

Each term in the brackets above belongs to I_1 which is an ideal *i.e.* $r \in R$ and $a_1 \in I_1 \Rightarrow r\,a_1 \in I_1$.

$\therefore \quad r\,p \in S$.

Similarly $p\,r \in S$ as in that case $a_2 \in I_2$ and $r \in R$

$\Rightarrow a_2\,r \in I_2$ which is an ideal.

Therefore S is both left and right ideal or simply an ideal.

§ 23. Principal Ideal. An ideal S generated by a single element a of the ring *i.e.* (a) is called a Principal Ideal, provided. **(Meerut M. Sc. 1969)**

if T be any other ideal of R containing a then it contains S *i.e.* $S \subseteq T$.

Unit Ideal. If R is a ring with unity then the ideal generated by 1 the unity element of R *i.e.* $(1)=R$ as any element r of the ring can be expressed as $r.1=r$. Hence the whole ring R is the ideal generated by 1 and is called unit ideal which is a principal ideal.

Null Ideal. The ideal generated by zero element of ring. R *i.e.* (0) will consist of only the zero element of ring R as $r\,0=0\ \forall\ r \in R$ and this ideal is called Null ideal which is a principal ideal.

From above we conclude that every ring (which must have zero element) will have at least one principal ideal *i.e.* the null ideal. In case the ring R be a ring with unity then it has at least two principal ideals *i.e.* the unit ideal and null ideal.

Theorem 25. *If a is an element of a commutative ring R with unity then the set $S=\{r\,a : r \in R\}$ is a principal ideal of R generated by the element a i.e. $S=(a)$.*

In order to prove that S is an ideal generated by single element a we have to prove the following

(i) $a \in S$.

(ii) S is an ideal of R.

(iil) S is smallest ideal containing a. In other words if T is any other ideal of R containing a then $S \subseteq T$.

Proof :—(i) a ∈ S.

Since the ring is with unity. $\therefore$ $1 \in R$.

Hence $1.a=a$. But $1.a \in S$ by definition.

$\therefore$ $a \in S$.

(ii) S is an ideal of R.

See proof of Theorem 23 (A) Page 251.

(iii) S is smallest ideal containing a.

Let ra be an element of S so that $r \in R$

Now if T is an ideal of R containing a then

$$a \in T, r \in R \Rightarrow r\,a \in T.$$

$$\therefore \quad r\,a \in S \Rightarrow r\,a \in T. \quad \therefore \quad S \subseteq T.$$

Hence S is a principal ideal of R generated by a.

Principal left ideal. In case the ring R be a ring with unity but **not commutative** then the set $S=\{r\,a : r \in R\}$ is the principal left ideal generated by a.

Similarly the set $S=\{a\,r : r \in R\}$ is the principal right, ideal generated by a.

When the ring is **commutative** then any principal left ideal will also be principal right ideal and as such it is termed only as principal ideal.

§ 24. Principal Ideal Ring.

Definition. *A ring for which every ideal is a principal ideal is called a principal ideal ring.*

(Raj. 67; Benares 61; Meerut 1969)

Exercise 8

1. *Every field is a principal ideal ring.*

Field is a commutative ring with unity without zero divisors.

From Theorem 22 P. 251 we know that a field has no proper ideals. In other words the only ideals it has are the null ideal and the unit ideal both of which are principal ideals. Thus every ideal of a field is a principal ideal and as such by definition field is a principal ideal ring.

2 *Consider the ring*

$$R=[(0, 1, 2, 3, 4), +_5, \times_5].$$

Is it a principal ideal ring ?

The above ring can be easily shown to be a field as in Ex. 2 P. 196 which has no proper ideals. The only ideals it will have will be null ideal and unit ideal both of which are principal ideals and as such it is a principal ideal ring.

Let us verify that it has no proper ideals

(0)=The principal ideal generated by $0=\{0\}$=Null ideal.

$(1)=(r.1 : r \in R)=\{0, 1, 2, 3, 4\}$=Unit ideal.

$(2)=(r.2 : r \in R)=\{0, 2, 4, 6, 8\}=\{0, 2, 4. 1, 3\}$
=Unit ideal.

$\because \quad 2\underset{\times_5}{\times}4=8=3 \qquad 2\underset{\times_5}{\times}3=6=1.$

$(3)=\{r.3 : r \in R)=\{0, 3, 6, 9, 12\}=\{0, 3, 1, 4, 2\}$
=Unit ideal.

$(4)=\{r.4 : r \in R)=\{0, 4, 8, 1\ , 16)=\{0, 4, 3, 2, 1\}$
=Unit ideal.

Thus the only ideals of ring R are Null ideal and unit ideal both of which are principal ideals and as such the ring R is a principal ideal ring.

3. *Find all the principal ideals of the ring.*

$$R=[(0, 1, 2, 3, 4, 5),_{+6}, \times_6].$$

Above is a commutative ring with unity. It is not a field as it is a ring with zero divisors and as such it will have ideals other than proper ideals and hence by Th. 25 P. 257 the set $S=\{r\,a : r \in R\}$ is a principal ideal generated by a and is denoted by (a).

As in Example (2) we can show that

$(0)=\{0\}$ Null ideal.

$(1)=\{0, 1, 2, 3, 4, 5\}$ Unit ideal.

$(2)=\{0, 2, 4, 6, 8, 10\}=\{0, 2, 4, 0, 2, 4\}=\{0, 2, 4\}$.

$(3)=\{0, 3, 6, 9, 12, 15\}=\{0, 3, 0, 3, 0, 3\}=\{0, 3\}$

Similarly

$(4)=\{0, 2, 4\}$, $(5)=\{0, 1, 2, 3, 4, 5\}=$Unit ideal.

Hence the principal ideals are

Null ideal, unit ideal, and ideal $\{0, 3\}$, ideal $\{0, 2, 4\}$

Theorem 26. *Let R be a commutative ring with unity and a, b be two non-zero elements of R then*

$(a)=(b) \Leftrightarrow$ *a and b are associates.*

a and b are associates if a/b and b/a

$(a)=$ Principal ideal generated by a

$\therefore \quad (a)=\{ax : x \in R\}$

Now $(a)=(b) \Rightarrow (a) \subseteq (b)$

$\Rightarrow a \in (b) \Rightarrow a=rb$ for some $r \in R$

$\Rightarrow b/a$ *i.e.* b is a divisor of a.

Similarly from $(b) \subseteq (a)$ we can prove a/b

Thus b/a and $a/b \Rightarrow a$ and b are associates.

Converse. given a/b, b/a, **to prove** $(a)=(b)$

$a/b \Rightarrow b=xa$ for some $x \in R$.

Again if u is an element of (b) then $u=yb$ for some $y \in R$

or $u=y(xa)=(yx)a=za$ when $z \in R$

$\Rightarrow u \in (a)$

Thus $u \in (b) \Rightarrow u \in (a)$ $\therefore$ $(b) \subseteq (a)$

Hence $a/b \Rightarrow (b) \subseteq (a)$

Similarly $b/a \Rightarrow (a) \subseteq (b)$

$\therefore$ $(a)=(b)$ **Proved.**

Theorem 27. *The ring of integers is a principal ideal domain.* **(Utkal 69; Lucknow 70; Benares 61; Meerut M. Sc. 67; Raj. M. Sc. 1969)**

Let $(I, +, .)$ be the ring of integers which is commutative ring with unity and without zero divisors and as such it is an integral domain. Now I will be a principal ideal ring (here principal ideal domain as the given ring is an integral domain) if every ideal in I is a principal ideal.

Choose S any ideal of the above ring I. In case S is a null ideal then it is a principal ideal.

Let us now suppose that S is not a null ideal *i.e.* $S \neq (0)$.

Now S contains at least one non zero integer say a and S being a sub group of I under addition. $\therefore$ $a \in S \Rightarrow -a \in S$. Hence we conclude that if $a \neq 0$ then S must contain at least one $+$ive integer as both a and $-a \in S$.

If a is $+$ive then $a \in S$ and if a is $-$ive then $-a$ is $+$ive and it belongs to S.

Let S_+ denote the set of all $+$ive integers in S and every set of $+$ive integers must have a least number. Choose K to be the least $+$ive integer of S_+. We will establish that S is the principal ideal generated by K *i.e.* $S=(K)$, and as such any ideal S will be a principal ideal being generated by a single element.

If x be any element of S then by division algorithim $\exists$ integers q and r such that

$$x=bq+r \qquad \text{where } 0 \leqslant r < b$$

or $$x-bq=r.$$

Now $b \in S, q \in I \Rightarrow bq \in S$ as S is an ideal.

Again $x \in S$ and $bq \in S \Rightarrow x-bq \in S$

as S is a sub group of I

$\therefore \quad r \in S$ because $x-bq=r.$

But $0 \leqslant r < b$ and b is the least +ive integer such that $b \in S$ and here we find that $r < b$ also $\in S$, which is a contradiction of b being least and therefore r must be zero.

Hence $x=bq.$

Above relation shows that every element of S is of the form bq *i.e.* $S=(bq : q \in R)$.

Therefore S is an ideal generated by b *i.e.* $S=(b)$ and as such it is a principal ideal. Since S was any principal ideal other than null ideal, it follows that every ideal $S \neq (0)$ is a principal ideal and as such the ring of integers is a principal ideal ring or principal ideal domain

§ 25. Maximal Ideal.

Definition. *An ideal $S \neq R$ in a ring R will be said to be a maximal ideal of R if whenever T is an ideal of R such that $S \subseteq T \subseteq R$ then either $S=T$ or $R=T$.*

In simple language above amounts to saying that ideal S will be maximal ideal if it is impossible to find another ideal which lies between S and the whole ring R.

Hence if S is a maximal ideal then there shall not exist any other ideal T properly contained in R and which properly contains S.

Illustration. Let R be a ring of integers and choose

$S=(6)=\{...-18, -12, -6, 0, 6, 12, 18,...\}$

But $T=(3)=\{...-18, -15, -12, -9, -6, -3, 0, 3, 6, 9, 12, 15, 18, ..\}$

Thus S is not a maximal ideal as there exists an ideal T which lies between S and R.

But if we choose $S=(5)=\{...-15, -10, -5, 0, 5, 10, 15,...\}$ then S is a maximal ideal because the only ideal containing S is R itself.

Theorem 28. *An ideal S of a ring I of integers is a maximal ideal if and only if S is generated by some prime integer.*

From Th. 27 P. 260 we know that every ideal of a ring of integers is a principal ideal which is generated by a single element. Choose ideal $S=(p)$ where p is +ive as ideal generated by $-p$ is same as that generated by p and hence we have taken p to be positive.

$S=(p)$ and we have to show that

S is maximal ideal $\Leftrightarrow$ p is prime.

Ist Case. Let p be prime and we will show that S is maximal ideal.

$S=(p)$ and let T be any other ideal of I. Since every ideal of I is a principal ideal as such let $T=(q)$

such that $S \subseteq T \subseteq I$

Now $S \subseteq T \Rightarrow (p) \subseteq T \Rightarrow p \in T$

$\Rightarrow p \in \{k\,q : k \in I\}$

$\Rightarrow p=rq$ where r is some +ive integer.

But p is prime therefore either $q=1$ or $q=p$

If $q=1$ then $T=(q)=(1)=I$

If $q=p$ then $T=(q)=(p)=S$

Thus $S \subseteq T \subseteq I \Rightarrow$ either $T=I$ or $T=S$.

Hence S is a maximal ideal.

2nd Case. S=(p) is a maximal ideal. To show that p is prime.

Let p be not prime then p must be composite and choose $p=xy$ when $x \neq p, \pm 1$, $y \neq p, \pm 1$

Clearly $(p) \subseteq (x) \subseteq I$ and (p) being maximal ideal it follows that either $(x)=(p)$ or $(x)=I$

If $(x)=I$ then $x=1$ which is a contradiction as $x \neq 1$.

If $(x)=(p)$, then x will be a multiple of p and let $x=kp$ for some integer k.

$\therefore \quad p=xy=kpy \quad \therefore \quad ky=1$ as $p \neq 0$

As both k and y are integers it follows from $ky=1$ that either $k=y=1$ or $k=y=-1 \quad \therefore \quad y=\pm 1$ which is again a contradiction. Hence p is not composite, it must be prime.

POLYNOMIAL RINGS

§ 26. Polynomial over a ring R.

Definition. *Let R be an arbitrary ring and x be any indeterminate symbol not belonging to R which commutes with every element of R then the expression of the form*

$$f(x)=a_0x^0+a_1x^1+a_2x^2+\ldots+a_nx^n=\sum_{r=0}^{n} a_rx^r$$

(Kanpur M. Sc. Stat. 69; Agra 70)

where the sum is taken over a finite number n of integers and $a_i \in R$ is called a polynomial of degree n in x over the ring R.

Another notation. The above polynomial can briefly be

expressed as $(a_0, a_1, a_2 \ldots a_n)$ *i.e.* if R be the ring of integers then the polynomial

$$3x^0-2x^1+5x^2=(3, -2, 5).$$

Similarly $(4, 3, -2, 0, 4)=4x^0+3x^1-2x^2+0x^3+4x^4$.

Equality of polynomials.

Two polynomials are said to be equal if and only if the coefficients of like powers of unknown are equal, *e g.*

$$(a_0, a_1, a_2, \ldots, a_n)=(b_0, b_1, b_2, \ldots, b_n),$$

if $$a_0=b_0, a_1=b_1, \ldots, a_n=b_n$$

$5+4x+7x^2-9x^3$ and $5+4y+7y^2-9y^3$

are equal polynomials over the ring of integers.

Sum of two polynomials.

$$f(x)=a_0x^0+a_1x^1+a_2x^2+\ldots+a_nx^n$$

$$g(x)=b_0x^0+b_1x^1+b_2x^2+\ldots+b_mx^m,$$

then the sum $f(x)+g(x)$ of the above two polynomials is defined as

$$f(x)+g(x)=(a_0+b_0)\,x^0+(a_1+b_1)\,x^1+(a_2+b_2)\,x^2+\ldots$$
$$+(a_m+b_m)\,x^m+\ldots+a_nx^n \text{ if } n>m$$

or $$(a_0+b_0)\,x^0+(a_1+b_1)\,x^1+\quad(a_n+b_n)\,x^n+\ldots+b_mx^m$$
$$\text{if } m>n,$$

i.e. $$(a_0, a_1, a_2, \ldots\ldots)+(b_0, b_1, b_2, \ldots)$$
$$=(a_0+b_0)+(a_1+b_1)+(a_2+b_2)+\ldots$$

The product of two polynomials.

$$f(x).g(x)=a_0b_0x^0+(a_0b_1+a_1b_0)\,x^1+(a_0b_2+a_1b_1+a_2b_0)\,x^2$$
$$+\ldots+a_nb_m\,x^{m+n}$$

$$=c_0x^0+c_1x^1+c_2x^2+\ldots\ldots$$

where $$c_r=a_0b_r+a_1b_{r-1}+\ldots+a_rb_0=\sum_{i+j=r} a_i\,b_j$$

Degree of polynomial.

The degree of polynomial $f(x)$ written before is n if $a_n\neq 0$ *i.e.* the exponent of highest power of x having non zero

coefficient and we write it as deg$f$ $(x)=n$, the coefficient a_n is called the leading coefficient.

Degree of sum and product of polynomials.

Let deg $f(x)=n$ and deg $g(x)=m$, then

$$\deg [f(x)+g(x)]=n \quad \text{if } n>m$$
$$=m \text{ if } m>n$$
$$=n \text{ if } m=n \text{ and } a_n+b_m\neq 0$$

and in case $a_n+b_m=0$, then the degree of sum will be less than n.

$$\deg [f(x).g(x)]=m+n \text{ if } a_nb_m\neq 0$$
$$< m+n \text{ if } a_nb_m=0.$$

Even if $a_n\neq 0$ $b_m\neq 0$ we can have $a_nb_m\neq 0$ or $a_nb_m=0$ as the ring R being arbitrary can be a ring without zero divisors or with zero divisors.

Ex. 1. *Consider the following polynomials over the ring* $(I_{,+6,\times 6})$

$f(x)=2+4x+2x^2 \qquad a_n=2$

$g(x)=$ (a) $2x+4x^2 \qquad b_m=4$

or (b) $2x+3x^2, \qquad b_m=3$

$h(x)=2+3x$

(a) deg $[f(x)+g(x)]$: One may be tempted to say that deg $[f(x)+g(x)]=2$

But Since $a_n+b_m=2\underset{+6}{+}4=0 \quad \therefore \quad \deg [f(x)+g(x)]\neq 2$

$$f(x)+g(x)=2+(4\underset{+6}{+}2)\,x+(2\underset{+6}{+}4)\,x^2=2+0x+0x^2$$

$\therefore$ deg $[f(x)+g(x)]=0$

(*b*) deg $[f(x).g(x)]$. Here also one may be tempted to say that the degree is 4.

But $a_nb_m=2.3=0$ *i.e.* $a_nb_m=0$ $\therefore$ deg $[f(x).g(x)]\neq 4$
$\times 6$

$$f(x).g(x)=(2+4x+2x^2)(2x+3x^2) \text{ [for}_{+6,\times 6}\text{]}$$
$$=4x+(2.3+4.2)x^2+(4.3+2.2)\,x^3+2.3\,x^4$$
$$=4x+(0+2)\,x^2+(0+4)\,x^3+0\,x^4$$
$$=4x+2x^2+4x^3$$

$\therefore$ deg $\{f(x).g(x)\}=3$

(c) $h(x).h(x)=(2+3x)(2+3x)$
$$=4+(3.2+2.3)\,x+(3.3)\,x^2$$
$$=4+(0+0)x+3x^2$$
$$=4+3x^2$$

$\therefore$ deg $\{h(x).\,h(x)\}=2$

§ 27. Isomorphism of a set of constant polynomials of R[x] on R.

Theorem 29. *If R is an arbitrary ring and R′ is the set of constant polynomials in R [x] then R′ is isomorphic to R.*

i.e. $R' \cong R$.

$R'=[ax^0+0x+0x^2+0x^3\ldots : a \in R]$.

Define $f : R \to R'$ such that $f(a)=ax^0+0x+0x^2\ldots$
$\forall\ a \in R$

f is one-one :

$$f(a)=f(b) \Rightarrow ax^0+0x+\ldots=bx^0+0x+\ldots$$
$$\Rightarrow a=b.$$

f is clearly onto.

f preserves the two compositions in R.

$$f(a+b)=(a+b)\,x^0+0x+0x^2+\ldots$$
$$=[ax^0+0x+0x^2+\ldots]+(bx^0+0x+0x^2+\ldots]$$
$$=f(a)+f(b).$$
$$f(a\,b)=abx^0+0x+0x^2+\ldots$$
$$=[ax^0+0x+0x^2\ldots]\,[bx^0+0x+0x^2+\ldots]$$
$$=f(a)\,f(b).$$

Hence f is an isomorphism of R onto R'

$$\therefore \quad R \cong R'$$

Since the relation of isomorphism is an equivalence relation.

$$\therefore \quad R' \cong R.$$

In view of the isomorphism we shall in future identify the constant polynomials in $R[x]$ with the element a of R *i.e.* $ax^0+0x^1+0x^2+\ldots\ldots$ will be written an a only.

Theorem 30. Ring of Polynomials.

The set of all polynomials over a ring R forms a ring with respect to addition and multiplication of polynomials. This ring is called the polynomial ring R [x] over the ring R.

Let $f(x)=\Sigma\, a_i x^i$, $g(x)=\Sigma\, b_k x^k$, $h(x)=\Sigma\, c_m x^m$ be three polynomials. We shall establish the three axioms R_1, R_2, R_3 of a ring.

R_1 The set of polynomials is an abelian group for addition.

Closure : The sum of two polynomials is again a polynomial.

Identity. The zero polynomial $0(x)=\Sigma\, a_r x^r$ in which all the coefficients a_r are zero (the zero of R) is the identity of the ring of polynomials.

Inverse. The additive inverse of the polynomial,

$$f(x)=a_0+a_1x+a_2x^2+\ldots+a_ix^i \text{ is}$$
$$-a_0-a_1x-a_2x^2-\ldots-a_ix^i$$

The **commutative and associative** property follows from those of R and hence an abelian group.

R_2 Multiplication is a binary operation which is associative.

We know that the product of two polynomials is again a polynomial and for associative we have to prove that

$$\{f(x).g(x)\}.h(x)=f(x).[g(x).h(x)]$$
$$f(x).g(x)=(\Sigma\, a_ix^i)\,(\Sigma\, b_kx^k)=\Sigma\, d_ix^i$$

where $d_i = \Sigma\, a_j b_k$ such that $j+k=i$.

$\therefore\ [f(x).g(x)]\,h(x) = (\Sigma\, d_i x^i)\ (\Sigma\, c_m x^m) = \Sigma\, e_l x^l$,

where $e_l = \Sigma\, d_i c_m,\ i+m=l$

$= \Sigma\ (\Sigma\, a_j b_k)\, c_m,\ j+k=i,\ i+m=l$

$= \Sigma\, a_j b_k c_m,\ j+k+m=l.$

Similarly we can show that

$$f(x)\,[g(x).h(x)] = \Sigma\, e_l x^l.$$

Hence multiplication is associative.

R_3 **Multiplication distributes addition.**

i.e. $f(x).[g(x)+h(x)] = f(x).g(x)+f(x).h(x)$,

L.H.S. $= (\Sigma\, a_j x^j)\ \{\Sigma\, b_k x^k + \Sigma\, c_k x^k\}$

$= (\Sigma\, a_j x^j)\ \{\Sigma\ (b_k+c_k)\ x^k\} = \Sigma\, e_l x^l$

where $e_l = \Sigma\, a_j\ (b_k+c_k) = \Sigma\, a_j b_k + \Sigma\, a_j c_k,\ j+k=l.$

R.H.S. $= (\Sigma\, a_j x^j)\ (\Sigma\, b_k x^k) + (\Sigma\, a_j x^j)\ (\Sigma\, c_k x^k)$

$= \Sigma\ (\Sigma\, a_j b_k)\ x^l + \Sigma\ (\Sigma\, a_j c_k)\ x^l,\ l=j+k$

$= \Sigma\ [\Sigma\, a_j b_k + \Sigma\ a_j c_k]\ x^l,\ j+k=l$

$= \Sigma\, e_l x^l$ = L.H.S.

Hence the distributive law holds.

Similarly we can show that

$[g(x)+h(x)]\ f(x) = g(x)\ f(x)+h(x).f(x).$

§ 28. If R is an integral domain so is R [x].

(Aligarh 66; Kanpur M.Sc. 69; Benares 69, 70; Allahabad 66, 69; Punjab 70)

For an integral domain we have to prove that it is a commutative ring with unity and without zero divisors,

$$f(x) \neq 0,\ g(x) \neq 0 \Rightarrow f(x).g(x) \neq 0.$$

Since R is an integral domain, it is a commutative ring and hence so is $R[x]$.

Again we may take $x^0 = 1$ as the unity element of integral domain, then the unity element of $R[x]$ is $1.x^0 = 1$.

Again we have to prove that $R[x]$ is a ring without zero divisors.

Let $f(x) \neq 0, g(x) \neq 0$ be two elements of the polynomial ring $R[x]$ whose coefficients are elements of R which is an integral domain If a_j and b_k be the leading coefficients of $f(x)$ and $g(x)$, then $a_j \neq 0$ and $b_k \neq 0$ and hence $a_j . b_k \neq 0$ as a_j and b_k are elements of an integral domain.

Again $a_j b_k$ is the coefficient of x^{j+k} in the product $f(x)\ g(x)$ and this coefficient is not zero and consequently $f(x) . g(x) \neq 0$.

Also we conclude that

$$\deg f(x) + \deg g(x) = \deg f(x) . \deg g(x) = j + k.$$

Therefore $R[x]$ has no zero divisors and hence $R[x]$ is an integral domain. This is denoted by $I(x)$ where I is the original integral domain.

Cor. I. In case R is a field then $R[x]$ must be an integral domain because every field is an integral domain. This is denoted by $F(x)$. **(Allahabad 66; Aligarh 66; Meerut B.Sc. Summer 69; Bombay 70)**

Here we have to gived the proofs of § 27 and § 28.

Theorem 31. *The polynomial domain* $F[x]$ *over a field is not a field.*

In case F be a field then it is necessarily an integral domain and the set of all polynomials over an integral domain F is an integral domain by § 28. Hence we have to prove that the set of all polynomials $F[x]$ where F is a field is not a field.

In order to prove $F[x]$ is not a field we have to establish that there exists at least one non zero element of $F[x]$ which does not possess a multiplicative inverse.

Let $g[x] \in F[x]$ such that deg $g[x]>0$.

The multiplicative identity of

$F[x]=1x^0=(1, 0, , 0, ..,0)$=unity polynomial whose degree is zero.

No zero polynomial can be multiplicative inverse of $g[x]$.

because $g[x].0[x]=0\neq$unity polynomial $(1, 0, 0, ..,0)$.

Hence let $h[x]\neq 0$ be the multiplicative inverse of $g[x]$

then deg $[g[x].h[x]]=$deg $[g[x]+h[x]]$

by § 28 as F is a field *i.e.* integral domain

But degree $g[x]>0$ and degree $h[x]>0$

$\therefore$ deg $[g[x].h[x]]>0$

Now we know that degree of unity polynomial is zero

$\therefore$ $g[x].h[x]$ can never be equal to unity polynomial as the degree of L.H.S. is greater than zero where as the degree of R.H.S is zero.

Hence $F[x]$ is not a field.

In fact the only inversible elements of $F[x]$ are constant polynomials excluding the zero polynomial. No other polynomial whose degree is greater than zero is inversible.

§ 29. Divisibility of polynomials over a field.

In case F be a field then the set of all polynomials $F[x]$ is an integral domain as, shown earlier. Choose $f(x)$, $g(x)$ to be any two elements of $F[x]$, then $f(x)$ is said to be a divisor of $g(x)$ if there exists a polynomial $h(x)$ in $F[x]$ such that

$$g(x)=f(x).h(x).$$

The statement $f(x)$ is a divisor of $g(x)$ is expressed symbolically as $f(x)| g(x)$

In case $f(x)/g(x)$ and $g(x)/f(x)$
then both $f(x)$ and $g(x)$ will be termed as **associates** and in that case $f(x)=c\ g(x)$ for some $c\neq 0 \in F$.

Units of F [x] : A unit of $F[x]$ is that element which has multiplicative inverse and we have shown in Th. 31 P. 269 that in the polynomial $F[x]$ the only inversible (multiplicatively) elements are constant polynomials.

Hence all constant polynomials in
$F[x]$ are units of $F[x]$.

Proper and improper divisors. Any polynomial $f(x)$ in $F[x]$ is divisible by its associate and units of polynomials in $F[x]$. Such divisors are **improper divisors** whereas all other divisors will be called **proper divisors**

Reducible and irreducible polynomials.

A polynomial $f(x)$ in $F[x]$ is called **reducible or composite** if it has proper divisors. Alternatively we may say that a polynomial $f(x)$ in $F[x]$ is **irreducible or prime** if it has no proper divisors.

i.e. $f(x)=g(x)\ h(x) \Rightarrow$ one of $g(x)$ or $h(x)$ is a unit in $F[x]$ *i.e.* one of them is a constant polynomials.

[Meerut M. Sc. 69]

It may be noted irreducibiliy of a polynomial depends on the character of the field.

For example the polynomial x^2+1 is irreducible over the field of reals whereas it will be reducible over the complex field.

as $x^2+1=(x+i)\ (x-i)$ where $x+i$, $x-i$ are polynomials of degree 1 each over the complex field.

Similarly the polynomial x^2-3 is irreducible over the field of rational numbers but is reducible over the field of real numbers as in that case

$$x^2-3=(x-\sqrt{3})\ (x+\sqrt{3}).$$

Monic polynomial. A polynominl $f(x)$ in $F[x]$ will be called a monic polynomial if the coefficient of highest power of x is equal to 1 the unity of the field F.

Thus the polynomial $5+4x-3x^2+x^3$ is a monic polynomial.

Greatest common divisor of two polynomials over a field.

The G. C. D. of the polynomials

$$f(x) \text{ and } g(x) \in F[x]$$

will be a polynomial $h(x)$ if

$$h(x) \mid f(x) \text{ and } h(x) \mid g(x)$$

and if there be any other polynomial $K(x)$ such that

$$K(x) \mid f(x) \text{ and } K(x) \mid g(x) \text{ then } K(x) \mid h(x)$$

The first condition implies that $h(x)$ is a common divisor and the second condition implies that it is greatest common divisor.

Relatively prime polynomials.

In case the greatest common divisor of

$$f(x),\ g(x) \in F[x]$$

be 1 the unity of field F then the two polynomials are said to be relatively prime. In this case $\exists$ polynomials $p(x)$ and $q(x)$ in $F(x)$

such that $$p(x) f(x) + q(x) g(x) = 1$$

Zeros of a polynomial : An element $a \in F$ will be called zero of polynomial

$$f(x) \in F[x] \text{ if } f(a)=0$$

i.e. zero of a polynomial x^2-7x+6 over the field of real is 6, 1.

§ 30. **Divison Algorithm for polynomials over a field F.**

Theorem 32. *Let $f(x)$ and $g(x) \neq 0$ be any two polynomials of the integral domain $F[x]$ over the field F, then there exists unique polynomials $q(x)$ and $r(x)$ in $F(x)$ such that*

$$f(x)=g(x)\, q(x)+r(x).$$

where r (x) is either zero or of degree less than that of g (x).

q (x) is called the quotient, r (x) the remainder over F.

[Bombay 70; Benares 65, 67, 70; Meerut M. Sc. 69; Allahabad 65]

Proof. Let $f(x)=a_0+a_1x+\ldots+a_nx^n$, $a_n\neq 0$

$g(x)=b_0+b_1x+\ldots+b_mx^m$, $b_m\neq 0$.

Ist case. deg f (x) < deg g (x), i.e n < m.

In this case $f(x)$ can be written as

$$f(x)=g(x).0+f(x)$$

so that $q(x)=0$ and $r(x)=f(x)$

Again if $f(x)=a_0$, $a_0\neq 0$ and **hence degree f (x) = 0.**

$\therefore$ $f(x)=0\cdot g(x)+a_0$ when degree $g(x) > 0$,

so that $q(x)=0$ and $r(x)=a_0$

or $f(x)=(a_0\, b_0^{-1})\, b_0+0$ when deg $g(x)=0$,

so that $q(x)=a_0\, b_0^{-1}$ and $r(x)=0$.

Hence the above theorem holds when degree $f(x)=0$ and degree $f(x) <$ deg $g(x)$.

2nd Case. Degree f (x) ⩾ degree g (x) i.e. n ⩾ m and n ⩾ 0.

We shall prove the theorem by the method of induction by assuming that the theorem holds when degree $f(x)$ is less than n and then show that the theorem is true when degree $f(x)=n$.

Now $f(x)=a_0+a_1x+a_2x^2+\ldots\ldots+a_{n-1}\,x^{n-1}+a_nx^n$

We rewrite $f(x)$ as under

$$f(x)=(a_nb_m^{-1})\,x^{n-m}\,(b_0+b_1x+\ldots+b_{m-1}x^{m-1}+b_mx^m)$$
$$+[(a_{n-1}-a_nb_m^{-1}\,b_{m-1})\,x^{n-1}+(a_{n-2}+a_nb_m^{-1}\,b_{m-2})\,x^{n-2}+\ldots]$$
$$=(a_nb_m^{-1}\,x^{n-m})\,g(x)+r_1(x) \text{ say} \qquad \ldots(1)$$

where degree $r_1(x)=n-1$ which is less than n.

On the assumption that the theorem holds for degree less than n we can apply the theorem on $r_1(x)$ whose degree $n-1$ is less than n

$\therefore \quad r_1(x)=g(x).h(x)+r(x)$ where deg $r(x)<$deg $g(x)$

Now putting the value of $r_1(x)$ in (1) we get

$$f(x)=[a_n b_m^{-1} x^{n-m}+h(x)].g(x)+r(x)$$

where deg.$r(x)<$ deg.$g(x)$

or $f(x)=q(x).g(x)+r(x)$ ...(2)

Hence the theorem holds good for $f(x)$ of degree (n).

Uniqueness of q (x) and r (x).

Let us suppose that

$$f(x)=q'(x)\ g(x)+r'(x) \quad \text{.. (3)}$$

where $r'(x)$ either zero or its degree is less than that of $g(x)$.

Hence from (2) and (3), we get

$$q(x).g(x)+r(x)=q'(x).g(x)+r'(x).$$

or $$[q(x)-q'(x)].g(x)=r'(x)-r(x)$$

Clearly the degree of L. H. S. is greater or equal to that of $g(x)$ if $q(x)-q'(x)\neq 0$ whereas the degree of R.H S. is either zero or less than that of $g(x)$. Hence the sign of equality will hold good when both of them become zero and it will be possible only when $q(x)-q'(x)=0$ as $g(x)\neq 0$,

and $$r'(x)-r(x)=0$$

or $$q'(x)=q(x) \text{ and } r'(x)=r(x)$$

Thus $q(x)$ and $r(x)$ are unique.

§ 31. Remainder Theorem.

If a polynomial $f(x)$ is divided by $(x-a)$, i e, a polynomial of degree 1 then the remainder is $f(a)$.

We know that

$$f(x)=g(x).q(x)+r(x)$$

where degree $r(x)<$ degree $g(x)$.

Choose $$g(x)=(x-a).$$

$$\therefore \quad f(x)=(x-a).q(x)+r(x)$$

where degree $r(x)<$ degree $g(x)$, *i.e.* <1, or degree $r(x)=0$ or say $r(x)=r$.

$$\therefore \quad f(x)=(x-a)\,q(x)+r.$$
$$\therefore \quad f(a)=(a-a)\,q(a)+r.$$

or $f(a)=r$=remainder when the polynomial $f(x)$ is divided by $x-a$. $\therefore \quad f(x)=(x-a)\,q(x)+f(a)$

Deduction. Factor Theorem.

A polynomial $f(x)$ is divisible by $(x-a)$ if and only if $f(a)=0$

[Allahabad 67; Meerut 71 (S)]

We have proved above that $f(x)=(x-a)\,q(x)+f(a)$.

$\therefore$ If $f(a)=0$ then $f(x)=(x-a)\,q(x)$ showing that $(x-a)$ is a factor of $f(x)$. Conversely if $(x-a)$ is a factor of $f(x)$, then

$$f(x)=(x-a)\,q(x),$$
$$\therefore \quad f(a)=(a-a)\,q(a)=0\cdot q(a)=0$$

Hence $f(a)=0$.

Example : *Prove that the polynomial* x^2+x+4 *is irreducible over* F *the field of integers modulo 11.*

(Meerut M. Sc. 1969)

A polynomial $f(x)$ is said to be irreducible if it has no proper divisors. Also by factor Theorem $(x-a)$ divides $f(x)$ iff $f(a)=0$. We shall evaluate $f(a)\ \forall\ a \in F$.

$$F=[\{0, 1, 2, \ldots\ldots 10\}_{+11}, \times_{11}]$$

If $a \in F$ then $a^2=a\times a \pmod{11}$

$$\therefore \quad f(0)=0^2+0+4=4\neq 0$$
$$f(1)=1^2+1+4=6\neq 0$$
$$f(2)=2^2+2+4=10\neq 0$$
$$f(3)=3^2+3+4=16_{+11}=5\neq 0$$
$$f(4)=4^2+4+4=5+4+4=13=2\neq 0$$

Similarly $f(5)=1, f(6)=2, f(7)=5, f(8)=10, f(9)=6,$ $f(10)=4$

Above relation shows that $\forall\ a \in F, f(a) \neq 0$ and hence none of the factors $x-a\ \forall\ a \in F$ divides $f(x)$. Therefore $f(x)$ has no proper divisors. It is therefore irreducible.

§ 32. Synthetic Division.

Let a polynomial $f(x)$ over a field F be divided by the polynomial $x-h$ then the quotient and the remainder are obtained by the process of synthetic division as explained below,

$$f(x)=a_0+a_1x+a_2x^2+\ldots a_{n-1}x^{n-1}+a_nx^n$$

and let $q(x)=b_0+b_1x+b_2x^2+\ldots b_{n-1}x^{n-1}$

be the quotient when $f(x)$ is divided by $x-h$ and the remainder be R which is of zero degree.

$$\therefore\ (a_0+a_1x+\ldots+a_{n-1}x^{n-1}+a_nx^n)$$
$$=(x-h)(b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1})+R.$$

$$\therefore\ a_n=b_{n-1} \quad \text{or} \quad b_{n-1}=a_n$$
$$a_{n-1}=-h\,b_{n-1}+b_{n-2} \quad \therefore\ b_{n-2}=a_{n-1}+h\,b_{n-1}$$
$$a_{n-2}=-h\,b_{n-2}+b_{n-3} \quad \therefore\ b_{n-3}=a_{n-2}+h\,b_{n-2}$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$
$$a_2=-h\,b_2+b_1 \quad \therefore\ b_1=a_2+h\,b_2$$
$$a_1=-h\,b_1+b_0 \quad \therefore\ b_0=a_1+h\,b_1$$
$$a_0=-h\,b_0+R \quad \therefore\ R=a_0+h\,b_0$$

The above process can be exhibited in tabular form as under

h |	a_n	a_{n-1}	.....	a_2	a_1	a_0
		$h\,b_{n-1}$	.....	b_2h	b_1h	hb_0
b_{n-1}		$a_{n-1}+hb_{n-1}=b_{n-2}$		$a_2+b_2h=b_1$	$a_1+b_1h=b_0$	$a_0+hb_0=R$

Rule. Write down the coefficients of the given polynomial starting with the coefficient of x^n, *i.e.* a_n which is also equal to b_{n-1}. Supply the coefficients of missing terms by zero. If the polynomial be divided by $x-h$ then write

h in the corner. Multiply each element of first line by h and write it below next and add, In the third line you will get the coefficients $b_{n-1}, b_{n-2}, b_{n-3}, \cdots, b_2, b_1, b_0$ and R.

The first coefficient b_{n-1} is the same as a_n. In case $R=0$ then $f(x)$ is divisible by $x-h$ otherwise R is the value of $f(x)$ for $x=h$, *i.e.* $R=f(h)$. If the divison is done by $x+h$, then write $-h$ in the corner and proceed as above.

Ex. 1. *Find the quotient and the remainder when,*

$f(x)=2x^4-3x^2-32x+6$ *is divided by* $x-3$.

$f(x)=2x^4+0x^3-5x^2-32x+6$

3 |	2	0	−5	−32	6
		6	18	39	21
	2	6	13	7 |	27=R

∴ quotient is $2x^3+6x^2+13x+7$ and remainder is 27.

Ex. 2. *In the field of residue classes modulo 5, find the quotient and remainder when* $f(x)=3x^3-4x^2+2x-2$ *is divided by* $x-3$.

Here the coefficients are elements of residue class field modulo 5.

3 |	3	−4	2	−2
		9=4	0	6=1
	3	0	2 |	−1=4

$9=4 \pmod 5$, $-1=4 \pmod 5$, $6=1 \pmod 5$.

∴ quotient is $3x^2+2$ and remainder is 4.

Theorem 33. *A polynomial domain* $F[x]$ *over a filed* F *is a principal ideal domain.* **(Lucknow 70; Kanpur M.Sc. stat. 71; Aligarh 66)**

From cor. I P. 269 we know that the polynomial domain $F[x]$ is an integral domain and as such it is a commutative ring with unity and without zero divisors. If it is to be a principal ideal ring we have to show that every ideal in $F[x]$ is a principal ideal

The proof is exactly similar to that of Th. 27 on Page 260 in which we showed **that the ring of integers is a principal ideal domain.**

Choose S any ideal of $F[x]$. If S is a null ideal *i.e.* an ideal generated by zero polynomial *i.e.* $S=(0)$ then it is a principal ideal as every null ideal is a principal ideal.

Let us now suppose that S is not a null ideal *i.e.* $S\neq(0)$, then there exists non zero polynomials in $F[x]$. Suppose $g(x)$ is a polynomial of lowest degree belonging to S and we shall establish that the ideal S is generated by $g(x)$ *i.e.* $S=(g(x))$.

Let $p(x)$ be an arbitrary polynomial in S then by division algorithm there exists two polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$$p(x)=g(x)\,q(x)+r(x) \qquad \ldots(1)$$

where $r(x)=0$ or deg. $r(x) <$ deg. $g(x)$

Now $q(x) \in F[x]$, $g(x) \in S$

$\Rightarrow g(x)\,q(x) \in S$ as S is an ideal

Also $p(x) \in S$, $g(x)\,q(x) \in S$.

$\Rightarrow p(x)-g(x)\,q(x) \in S$ as S is a sub group of $F[x]$.

$\Rightarrow r(x) \in S$ from I.

Now either $r(x)=0$ or deg $r(x) <$ deg. $g(x)$

The second possibility is ruled out because $g(x)$ is a polynomial of lowest degree in S and $r(x) \in S$ cannot be a polynomial such that

$$\deg r(x) < \deg g(x)$$

Hence we must have $r(x)=0$

Therefore $p(x)=g(x)\,q(x)$

Above relation shows that every polynomial in S is of the form $g(x)\,q(x)$.

i e. $S=g(x)\,q(x) \because q(x) \in F[x]$

Therefore S is an ideal generated by $g(x)$ *i.e* $S=(g(x))$ and as such it is a principal ideal. Since S was any ideal other than null ideal, it follows that every ideal which is not a null ideal is a principal ideal. Hence $F[x]$ is a principal ideal ring [domain]

Theorem 34. *The polynomial ring $I[x]$ over the ring of integers is not a principal ideal ring.* **(Meerut M. Sc. 1967)**

Here we shall establish that any ideal is not a principal ideal and hence $I[x]$ is not a principal ideal ring.

Consider the ideal $(2, x)$ of the ring $I[x]$ generated by two elements 2 and x of $I[x]$. We shall show that it is not a principal ideal.

If possible let $(2, x)$ be a principal ideal in $I[x]$ then $\exists$ a non zero polynomial $g(x)$ in $I(x)$ which generates the ideal $(2, x)$,

i e. $(2, x)=(g(x))$.

Now $2 \in (g(x))$ and $x \in (g(x))$, therefore $\exists$ polynomials $a(x)$ and $b(x)$ is $I[x]$ such that $2=a(x)\,g(x)$. ...(1)

$x=b(x)\,g(x)$ .. (2)

But $I[x]$ is an integral domain and hence

deg. $a(x)\,g(x)$ = deg. $a(x)$ + deg. $g(x)$ = deg. $2=0$...(3)

deg. $b(x)\,g(x)$ = deg. $b(x)$ + deg. $g(x)$ = deg. $x=1$...(4)

From (3) deg $a(x)=0$, deg. $g(x)=0$ *i.e.* both $a(x)$ and $g(x)$ are constant polynomials and because $a(x)\,g(x)=2$ we can have the following four possibilities of choosing $a(x)$ and $g(x)$.

$a(x)=1,\ g(x)=2$ $\qquad$ $a(x)=-1,\ g(x)=-2$

$a(x)=2,\ g(x)=1$ $\qquad$ $a(x)=-2,\ g(x)=-1$.

In case $g(x)=1$ or -1 we have

$(g(x))=I[x]$ which contradicts that $(2, x)=(g(x))$

as $I[x]\neq(2, x)$

Again if $g(x)=+2$ or -2 then form (2) we get

$x=\pm 2$, $b(x)=\pm 2(c_0+c_1x+c_2x^2+\ldots)$ where $c_i \in I$

Above relation implies that $c_0=0$, $c_2=c_3=\ldots=0$

and c_1 should satisfy the relation $1=\pm 2c_1$ where c_1 is an integer.

This too is not possible as there cannot be any integer c_1 satisfying this relation.

Hence $(2, x)$ cannot be a principal ideal. Therefore $I[x]$ is not a principal ideal ring

§ 33. Greatest common divisor.

Definition. *Let $f(x)$ and $g(x)$ be any two polynomials in $F[x]$. Then greatest common divisor (g. c d.) of $f(x)$ and $g(x)$ is a polynomial $d(x)$ satisfying the following properties*

(i) $d(x)/f(x)$, $d(x)/g(x)$

(ii) If $c(x)/f(x)$, $c(x)/g(x)$ *then* $c(x)/d(x)$.

§ 34. Euclidean Algorithm for polynomials over a field.

Theorem 35. *Let $f(x)$ and $g(x$ be any two polynomials in $F[x]$ not both of which are zero. Then $f(x)$ and $g(x)$ have a g c. d. $d(x)$ which can be expressed in the form*

$$d(x)=p(x)f(x)+q(x)g(x)$$

where $p(x)$ and $q(x)$ are polynomias in $F[x]$.

Proof. Choose the set S as under.

$S=\{m(x)f(x)+n(x)g(x) : m(x), n(x) \in F[x]\}$...(A)

We shall show that S is an ideal of $F[x]$ by using criteria on P. 246.

i.e. (i) $a-b \in S \quad \forall\ a, b \in S$

(ii) $rs \in S \quad \forall\ r \in R$ and $s \in S$

Let $a_1 = m_1(x) f(x) + n_1(x) g(x) \in S$

$a_2 = m_2(x) f(x) + n_2(x) g(x) \in S$

then $a_1 - a_2 = [m_1(x) - m_2(x)] f(x) + [n_1(x) - n_2(x)] g(x)$ also $\in S$

as $m_1(x) - m_2(x) \in F[x]$ and $n_1(x) - n_2(x) \in F[x]$

Again if $a(x)$ is any element of $F[x]$ then

$aa_1 = a(x)[m_1(x) f(x) + n_1(x) g(x)]$

$= [a(x) m_1(x)] f(x) + [a(x) n_1(x)] g(x)$ also $\in S$

Hence S is an ideal of $F[x]$.

Again from theorem 33 P. 277 we know that every ideal of $F[x]$ is a principal ideal and hence there exists an element $d(x)$ in S such that every element in S is a multiple of $d(x)$ by def. of principal ideal.

Now $d(x) \in S$ and hence by definition of S there will be polynomials $p(x)$ and $q(x)$ in $F[x]$ such that

$$d(x) = p(x) f(x) + q(x) g(x) \quad \ldots(i)$$

Again $F[x]$ is a ring with unity and hence putting $m(x) = 1$, $n(x) = 0$ $m(A)$ we get $f(x) \in S$. Again putting $m(x) = 0$, $n(x) = 1$ we get $g(x) \in S$.

Since $f(x)$ and $g(x)$ both $\in S$ and as proved earlier each of these is a multiple of $d(x)$ or $d(x)$ divides both $f(x)$ and $g(x)$.

Thus $d(x) / f(x)$, $d(x) / g(x)$

Again if $c(x) / f(x)$ and $c(x) / g(x)$ then

$c(x) / p(x) f(x)$ and $c(x) / q(x) g(x)$

or $c(x) / p(x) f(x) + q(x) g(x)$

or $c(x) / d(x)$

Hence by definition of greatest common divisor, $d(x)$ is the $g.c.d.$

LIST OF IMPORTENT QUESTIONS

List of Important questions and articles.

§ 1 P. 168, Excereise **1 P. 169** Q. [2, 3, 4]. § 2 P. 176, § 3 P. 177.

Excercise **2 P. 180** Q. [2, 5, 6, 7, 9, 10]. Th. 1 P. 192, § 5 P. 193 § 6 P. 195,

Excercise **3 P. 196** Q. [2, 3, 5, 8]. Th. 3 P. 204, Th. 4 P. 206, Th. 5 P. 207. Ex. I P. 209, Ex. 1, 2 P. 215–216, § 13 P. 218, Excercise 5 P. 225 Q. [2, 3, 4] Th. 11 P. 227, Th 15 P. 233, Th. 16 P. 234, § 19 P. 236–240 (Imp).

Th. 18 (A, B) P. 242, § 20 P. 245, Th. (19 A, B, 20, 21 A, B) P. 250. Excercise 7 P. 253 Q. [1, 2, 3].

§ 24 P. 257, Theorem 27 P. 260, § 28 P. 268

§30 P. 272, Th. 33 P. 277, Th. 34 P. 279.

CHAPTER IV
VECTOR SPACES

§ 1. Introduction. Let P and Q be the points (a, b) and (c, d) and the vectors

$$\vec{OP}=\alpha=(a, b) \text{ and } \vec{OQ}=\beta=(c, d) \text{ in } R\times R,$$

then by a vector 3α we mean $(3a, 3b)$ and by -2α we mean $(-2a, -2b)$.

Also $\alpha+\beta=(a+c, b+d)$ is defined as the vector addition and is the resultant of two forces represented by $\vec{OP}$ and $\vec{OQ}$ and is given by parallelogram law of forces by the diagonal $\vec{OR}$ of the parallelogram whose adjacent sides are OP and OQ.

Also we know fully well that

1. (a) $\alpha+\beta=\beta+\alpha$, *i e.* addition of vectors is commutative.

   (b) $(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma)$, *i.e.* addition of vectors is associative.

   (c) The zero vector $=(0, 0)$ is the identity element.

   (d) For vector $\alpha=(a, b)$ there exists a vector
   $$-\alpha=(-a, -b),$$
   such that $\alpha+(-\alpha)=(0, 0)=$ Identity
   Hence the inverse of every vector exists.

Also addition of vectors is a binary operation because sum of two vectors is again a vector.

All the above can be summed up in one sentence by saying that the set of vectors V forms an abelian group w.r.t. addition of vectors as the composition.

2. Also we know that multiplication of vectors by scalars satisfies the following laws, *i.e.* $\forall$ a, b as scalars and α, β as vectors we have

(a) $a(\alpha+\beta)=a\alpha+a\beta$.

(b) $(a+b)\alpha=a\alpha+b\alpha$.

(c) $(ab)\alpha=a(b\alpha)$

(d) $1.\alpha=\alpha$.

Internal and external composition.

We are acquainted with a binary composition in a set V which we have defined as a mapping of $V\times V\to V$. This may be called as an internal composition. This mapping associates to each pair of members of V, a member of V.

Again if V and F be two non empty sets then a mapping $f: V\times F \to V$ is called an external composition in V over F. This mapping associates to each pair of members of V and F a member of V.

For example in the set of matrices addition and multiplication is an internal composition because the sum and product of two matrices is again a matrix. On the other hand multiplication of a matrix by a scalar is an external composition because $aA=B$ where A and B are matrices and a is a scalar.

Notation for addition and multiplication.

Since we have to deal with four types of operations, *i.e.*,

(1) Addition of vectors, symbol $\oplus$

(2) Addition of scalars, symbol-+

(3) Multiplication of vectors by scalars, symbol *

(4) Multiplication of scalars, symbol.

But in actual practice for the sake of convenience we shall use the same symbol + both for addition of vectors

and addition of scalars and we shall not use any symbol for multiplication, *i.e.* $a * \alpha$ will be written as $a\,\alpha$ and $a.b$ will be written as ab.

§2. Vector space over a field F.

Let $(F, +, .)$ *be a field* (*whose elements will be termed as scalars*) *and* V *be a non empty set of elements called vectors. Again if there be an internal binary composition* $\oplus$ *and an external composition in* V *over* F * *which is called scalar multiplication satisfying the following axioms* $\forall\ \alpha, \beta \in V$ *and* $a, b \in F$. **(B.H.U. 70; Punjab 66, Meerut 68)**

1. $(V, \oplus)$ or $(V; +)$ **is an abelian group.**

i.e. closure property, associative, existence of identity and inverse, commutative.

2. **The multiplication of vectors by scalars satisfies the following :**

(a) $a * [\alpha \oplus \beta] = a * \alpha \oplus a * \beta$

or $a\,(\alpha+\beta) = a\alpha + a\beta$.

i.e., multiplication by a scalar is distributive w.r.t. vector addition.

(*b*) $(a+b) * \alpha = [\alpha * \alpha] \oplus [b * \alpha]$

or $(a+b)\,\alpha = a\alpha + b\alpha$,

i.e., multiplication by a vector is distributive w.r.t. scalar addition.

(c) $(a\ .\ b) * \alpha = a * (b * \alpha)$

or $(a\,b)\,\alpha = a\,(b\,\alpha)$.

i.e. multiplication by scalar is associative.

(d) $1 * \alpha = \alpha$, where 1 is the unit element of F or the multiplicative identity of the field F.

or $1\ \alpha = \alpha$.

Then the set V is called a vector space over the field F and is denoted as $V\ (F)$.

Note. From above definition we conclude that vector space $V(F)$ is a group on which the elements of a field operate in accordance with the rules given by (2) above. The element of F combined with an element of V gives rise to an element of V.

If we choose the field F as the field R of real numbers, a field C of complex numbers or a field Q of rational numbers, then V is called a real, complex or rational vector space.

Null space : *A vector space which has only one element the additive identity* **0** *is called null space or zero vector space and is denoted as* {**0**}

Important Note :

Whenever a scalar is multiplied by a vector the result is a vector. There will be two types of zero elements, one is zero vector denoted as bold type **0** which is an element of V and the other is zero scalar denoted as ordinary 0 which is an element of F. Generally the elements of V *i.e.* vectors will be denoted by $\alpha, \beta, \gamma, \ldots$ whereas the elements of F *i.e.* scalars will be denoted by $a, b, c, \ldots\ldots$

Excercise I

1. *Classify the various operations of addition and multiplication in the following statements.*

1 $a(\alpha+\beta)=a\alpha+a\beta$

$+$ on either side stands for addition of vectors, in $a\alpha$ multiplication stands for scalar multiplication.

2. $(a+b)\alpha=a\alpha+b\alpha$

$+$ on left stands addition in field F, $+$ on right stands for addition in V

3. $(a\ b)\ \alpha = a\ (b\ \alpha)$

multiplication in ab stands for multiplication in the field F whereas in $(ab)\ \alpha$ and $b\alpha$ it stands for scalar multiplication. Again $a\ (b\ \alpha)$ is also scalar multiplication of scalar a with vector $b\alpha$.

2. *Let V be the set of all ordered n-tuples of the elements of any field F for a fixed integer n, i.e.* (Delhi 69)

$$V=\{(a_1, a_2, \ldots, a_n) : a_i \in F\},$$

then V is a vector space over F with the following definitions.

i.e., $\alpha=(a_1, a_2, \ldots, a_n)$ and $\beta=(b_1, b_2, \ldots, b_n)$, then

1. $\alpha+\beta=(a_1+b_1, a_2+b_2, \ldots\ldots, a_n+b_n)$.

Addition of vectors

2. $a\alpha=(aa_1, aa_2, \ldots, aa_n)$.

Scalar multiplication of vectors.

3. $\alpha=\beta$ if $a_i=b_i$ for each $i=1, 2, \ldots, n$.

Equality of vectors.

With the above definitions we shall show that all the axioms of a vector space are satisfied.

1. $(V, +)$ is an abelian group.

(a) If $\alpha, \beta \in V$ then $\alpha+\beta$ as defined above is again a vector $\in V$ and hence closure property.

(b) $$(\alpha+\beta)+\gamma=[(a_1+b_1)+c_1,\ (a_2+b_2)+c_2,\ \ldots.]$$
$$=[a_1+(b_1+c_1),\ a_2+(b_2+c_2), \ldots]$$
$$=\alpha+(\beta+\gamma).$$

Because a_i, b_i, c_i being the elements of a field obey the associative law.

(c) The vector $\mathbf{0}=(0, 0, 0, \ldots, 0)$ is the identity element.

(d) For every vector $\alpha \in V\ \exists$ a vector

$$-\alpha=(-a_1, -a_2, \ldots, -a_n),$$

such that $\alpha+(-\alpha)=[a_1+(-a_1), a_2+(-a_2),...]$
$=[0, 0, 0, ..., 0]=\mathbf{0}=$identity.

i.e. inverse of every element exists and belongs to V.

(e' Again $\alpha+\beta=[a_1+b_1, a_2+b_2, ..., a_n+b_n]$
$=[b_1+a_1, b_2+a_2, ..., b_n+a_n]$
$=\beta+\alpha$ and hence commutative.

Therefore $(V, +)$ is an abelian group.

(2) Laws of scalar multiplication.

(1) $a(\alpha+\beta)=a\alpha+a\beta$.

$a(\alpha+\beta)=a(a_1+b_1, a_2+b_2, ...)$ by def.
$\{a(a_1+b_1), a(a_2+b_2), ...\}$ by def.
$=(aa_1+ab_1, aa_2+ab_2, ...)$ by R.D. Law in F.
$=(aa_1, aa_2, ..)+(ab_1, ab_2, ...)$ by def.
$=a(a_1, a_2, ...)+a(b_1, b_2, ...)$ by def.
$=a\alpha+a\beta$.

$(a+b)\alpha=(a+b)[a_1, a_2, ..., a_n]$ a, b, a_i's $\in F$
$=[(a+b)a_1, (a+b)a_2, ..., (a+b)a_n]$
$=[(aa_1+ba_1), (aa_2+ba_2), ..., (aa_n+ba_n)]$ by L D. Law in F.
$=(aa_1, aa_2, ..., aa_n)+(ba_1, ba_2, ... , ba_n)$ by def.
$=a(a_1, a_2, -....., a_n)+b(a_1, a_2,....., a_n)$ by def.
$=a\alpha+b\alpha$.

$(ab)\alpha=ab(a_1, a_2, ... a_n)$
$=((ab)a_1, (ab)a_2, ..., (ab)a_n)$
$=(a(ba_1), a(ba_2), ..., a(ba_n))$ by associatively in F.
$=a(ba_1, ba_2, ..., ba_n)$
$=a(b(a_1, a_2, ..., a_n))$
$=a(b\alpha)$

$1.\alpha.$ $=1(a_1, a_2, ..., a_n)$
$=(1.a_1, 1.a_2, ..., 1.a_n)$
$=(a_1, a_2, ..., a_n)=\alpha$.

As 1 is the unity of the field and hence $1 . a_i = a_i \ \forall \ a_i \in F$.

Hence the set V is a vector space over F and it is generally expressed as $V_n(F)$.

Similarly $V_2(F)$ is a vector space whose elements are ordered pairs $(a_1, a_2) : a_1, a_2 \in F$ and similarly $V_3(F)$ is a vector space whose elements are ordered triplets.

$(a_1, a_2, a_3) : a_1, a_2, a_3 \in F$.

3. *Prove that the set of all real valued continuous (differentiable or integrable) functions of x defined in some interval $[0, 1]$ is a vector space.*

Let V be the set of all such functions and f and g be any two functions of this set. We may define addition and scalar multiplication as under

$$(f+g)\ x = f(x) + g(x), \ \forall \ f, g \in V, \qquad \ldots(A)$$

$$(af)\ x = a . f(x). \qquad \forall \ a \in R \text{ and } f \in V \qquad \ldots(B)$$

1. (V, +) is an abelian group.

1. **Closure :** The sum of two continuous functions is again a continuous function.

2. **Associative :** $[(f+g)+h]\ x = (f+g)\ x + h(x)$ by def.

$$= [f(x) + g(x)] + h(x).$$

But $f(x)$, $g(x)$, $h(x)$ are real numbers and addition of real numbers is associative and hence

$$= f(x) + [g(x) + h(x)]$$
$$= f(x) + [(g+h)\ x]$$
$$= [f + (g+h)]\ x$$

$\therefore \ (f+g)+h = f+(g+h). \qquad \forall \ f, g, h \in R.$

Hence associative

3. **Identity :** The function O defined as $O(x) = 0$ is the identity of the set R.

$\because \ (O+f)\ x = O(x) + f(x) = 0 + f(x) = f(x).$

$\therefore \ O + f = f.$

Similarly $f+O=f$.

4. **Inverse :** The function $-f$ such that $(-f)\,x=-[f(x)]$ is the additive inverse of f.

$\because\ [(-f)+f]\,x=(-f)\,(x)+f(x)=-f(x)+f(x)$.
$=0=O(x)$

$\therefore\ (-f)+f=O$ the identity.

5. **Commutative.** $(f+g)\,x=f(x)+g(x)$
$=g(x)+f(x)$ as addition of
$=(g+f)\,x$ real numbers is commutative.

$\therefore\ f+g=g+f$.

2. Laws of scalar multiplication.

1. $[a\,(f+g)]=af+ag$.

$[a\,(f+g)]\,x=a\,[(f+g)\,x]$ by **B.**
$=a\,[f(x)+g(x)]$ by **A**
$=af(x)+ag(x)=(af)\,x+(ag)\,x$
$=(af+ag)\,x$.

$\therefore\ a\,(f+g)=af+ag$.

2. $(a+b)\,f=af+bf$

$[(a+b)\,f]\,x=(a+b)\,f(x)=af(x)+bf(x)$
$=(af)\,x+(bf)\,x=(af+bf)\,x$.

$\therefore\ (a+b)\,f=af+bf$.

3. $(ab)\,f=a\,(bf)$

$[(ab)\,f]\,x=abf(x)=a\,[bf(x)]$
$=a\,[(bf)\,x]=[a\,(bf)]\,x$.

$\therefore\ (ab)\,f=a\,(bf)$.

4. $1\,f=f$.

$(1.f)\,x=1.f(x)=f(x)$.

$\therefore\ 1.f=f$.

Thus all the postulates of a vector space are satisfied.

4. *A field F can be regarded as a vector space over any sub field S of F* **(Meerut 69)**

$(F, +, .)$ is a field whose elements are to be regarded as vectors and S is a sub field whose elements are to be regarded as scalars. Since S is a sub field therefore elements of S are also elements of F. the composition of scalar multiplication is the same as the composition of multiplication in $(F, +, .)$

Properties of vector space.

1. $(F, +)$ is an additive abelian group by definition.
2. Laws of scalar multiplication

$$a(\alpha+\beta)=a\alpha+a\beta$$

$$(a+b)\alpha=a\alpha+b\alpha$$

both these follow from R. D. Law and L. D. Law in a field as all a, b, α, β belong to F.

$$(ab)\alpha=a(b\alpha)$$

It follows from the fact that multiplication is associative in a field

$$1.\alpha=\alpha \quad \forall \quad \alpha \in F$$

1 is the unity element of sub field S which is also unity element of F and from definition

$$1.\alpha=\alpha \quad \forall \quad \alpha \in F$$

Hence F is a vector space over a sub-field S.

Cor. F is a vector space over F where F is any field, and hence **C is a vector space over C and R is a vector space over C.**

Cor. C is a field of complex numbers and R is a sub-field of C so that C **is a vector space over R**

Cor. R is not a vector space over C

Here real numbers are vectors where as complx numbers are scalars and scalar multiplication of a vector should be a

vector. But we know that the product of real number (vector) with a complex number (scalar) is not necessarily a real number (vector) *i.e.* R is not closed for scalar multiplication.

5. *The set $F(x)$ of all polynomials over a field F is a vector space w. r. t. vector addition as addition of polynomials and scalar multiplication as the product of a polynomial of zero degree, i e. an element of F.*

6. *The set of all convergent sequences is a vector space over the field of real numbers,*

Let $\alpha=\{\alpha_1, \alpha_2, \ldots,\alpha_n\}=\{\alpha_n\}$

$\beta=\{\beta_1, \beta_2, \ldots\beta_n\}=\{\beta_n\}$ be two convergent sequences.

1. $(V,+)$ **is an abelian group.**

(a) $\alpha+\beta=\{\alpha_n\}+\{\beta_n\}=\{\alpha_n+\beta_n\}$ and this is also a convergent sequence.

(b) $$\begin{aligned}\alpha+(\beta+\gamma)&=\{\alpha_n\}+[\{\beta_n\}+\{\gamma_n\}]=\{\alpha_n\}+\{\beta_n+\gamma_n\}\\&=\{\alpha_n+\beta_n\}+\{\gamma_n\}=[\{\alpha_n\}+\{\beta_n\}]+\{\gamma_n\}\\&=(\alpha+\beta)+\gamma.\end{aligned}$$

(c) **Identity.** $\{0\}=\{0, 0, 0, \ldots0\}$ is the identity.

(d) **Inverse.** For every sequence $\{\alpha_n\}$ there exists a sequence $\{-\alpha_n\}$, such that

$$\{\alpha_n\}+\{-\alpha_n\}=\{\alpha_n-\alpha_n\}=\{0\}=\text{identity}$$

(e) **Commutative.**

$$\begin{aligned}\alpha+\beta=\{\alpha_n\}+\{\beta_n\}&=\{\alpha_n+\beta_n\}=\{\beta_n+\alpha_n\}\\&=[\{\beta_n\}+\{\alpha_n\}]=\beta+\alpha.\end{aligned}$$

Laws of scalar multiplication

(i) $$\begin{aligned}a(\alpha+\beta)&=a[\{\alpha_n\}+\{\beta_n\}]=a\{\alpha_n+\beta_n\}\\&=\{a\alpha_n+a\beta_n\}=\{a\alpha_n\}+\{a\beta_n\}\\&=a\{\alpha_n\}+a\{\beta_n\}=a\alpha+a\beta.\end{aligned}$$

(ii) $(a+b)\,\alpha=(a+b)\,\{\alpha_n\}=\{(a+b)\,\alpha_n\}$
$=\{a\alpha_n+b\alpha_n\}=\{a\alpha_n\}+\{b\alpha_n\}$
$=a\,\{\alpha_n\}+b\,\{\alpha_n\}=a\alpha+b\alpha.$

(iii) $(ab)\,\alpha=ab\,\{\alpha_n\}=\{ab\alpha_n\}=a\,(b\alpha_n\}$
$=a\,(b\alpha).$

(iv) $1.\alpha=1.\{\alpha_n\}=\{1.\alpha_n\}=\{\alpha_n\}=\alpha.$

7. *The set of all $m\times n$ matrices with elements as real numbers is a vector space over the field of real numbers.*
(Meerut M. Sc. 67)

We have already shown in the chapter of groups that the set of all $m\times n$ matrices with real numbers is an additive abelian group.

Also the product of a matrix A (vector) by a real number a (scalar) is again a matrix *i.e.* (vector).

Also $a\,(A+B)=aA+aB$

$(a+b)\,A=aA+bA$

$(ab)\,A=a\,(bA)$ and $1A=A.$

Therefore $V\,(R)$ is a vector space.

8. *Examine whether the set V of all ordered pairs of integers form a vector space over the field R of real numbers, assuming the sum of ordered pairs and scalar multiplication as Ex 1 P. 288.*

For a vector space there is an external composition called scalar multiplication giving rise to a vector. In this vectors are ordered pair of integers say $(7, 5) \in V$ and let us choose a scalar $\frac{1}{3} \in R$.

But $\frac{1}{3}\,(7, 5)=(\frac{7}{3}, \frac{5}{3})$ by definition.

Now $(\frac{7}{3}, \frac{5}{3})$ does not belong to V as $\frac{7}{3}$ and $\frac{5}{3}$ are not integers. Hence it is not necessarily a vector space. If

however we choose the field as 1 of integers, then in that case it will be a vector space.

9. *Examine the following for vector space.*

$$V=\{(a, b) : a, b \in R\} \text{ and } F=R.$$

The addition and scalar multiplicatioh dəfined as given in each part.

(a) $(a, b)+(c, d)=(0, b+d)$

$$t\,(a, b)=(ta, tb) \quad t \in R.$$

Even if any of the postulates of a vector space is not satisfied, then it will not be a vector space. First of all $(V, +)$ has got to be additive abelian group for which identity element $(0, 0)$ must exist, such that

$$(a, b)+(0, 0)=(a, b).$$

But by definition,

$$(a, b)+(0, 0)=(0, b+0)=(0, b)\neq(a, b),$$

Even if we take (c, d) as the identity element then

$$(a, b)+(c, d)=(0, b+d)\neq(a, b).$$

Hence identity element does not exist and as such it is not even a group what to talk of vector space.

(b) $(a, b)+(c, d)=(a+c, b+d)$

$k\,(a, b)=(ka, b)$, $k \in R$ By definition.

Here $(V,+)$ will be an additive abelian group but laws of scalar multiplication for a vector space will not hold.

e.g. $$(a+b)\,\alpha=a\alpha+b\alpha.$$

Here $(k+k')\,(a, b)=[(k+k')\,a, b]$ by def. ...(1)

Also $k\,(a, b)+k'\,(a, b)=(ka, b)+(k'a, b)$ by def.

$=(ka+k'a, b+b)$ by def.

$=[(k+k')\,a, 2b]$. ...(2)

Hence from (1) and (2) we conclude that

$$(k+k')\,(a, b)\neq k\,(a, b)+k'\,(a, b).$$

Therefore $V(R)$ is not a vector space.

(c) $(a, b)+(c, d)=(a+c, b+d)$

$k(a, b)=(|k|a, |k|b)$ by def.

Let us verify whether

$(a+b)\alpha=a\alpha+b\alpha$, $\forall\ a, b \in F$ and $\alpha \in V$,

$(k+k')(a, b)=[|k+k'|a, |k+k'|b]$ by def. ...(1)

$$k(a, b)+k'(a, b)=(|k|a, |k|b)+(|k'|a, |k'|b)$$
$$=(|k|a+|k'|a, |k|b+|k'|b)$$
$$=[\{|k|+|k'|\}a, \{|k|+|k'|\}b].$$

.. (2)

Since $|k+k'| \leqslant |k|+|k'|$ and hence from (1) and (2) we conclude that $(k+k')(a, b) \neq k(a, b)+k'(a, b)$

Therefore $V(R)$ is not a vector space

(d) $(a, b)+(c, d)=(a+c, b+d)$,

$k(a, b)=(0, kb)$.

We know that one of the laws of scalar multiplication is that $1.\alpha=\alpha$, $\alpha \in V$.

Here $1.(a, b)=(0, b)$ be def.

But as $(0\ b) \neq (a, b)$ and hence $1\ \alpha \neq \alpha$.

Hence V is not a vector space over R.

(e) $(a, b)+(c, d)=(a+c, b+d)$

$k(a, b)=(k^2a, k^2b)$

We know that according to laws of scalar multiplication.

$(k+k')\alpha=k\alpha+k'\alpha$. $k, k' \in R, \alpha \in V$

$(k+k')(a, b)=k(a, b)+k'(a, b)$

R. H. S. $=(k^2a, k^2b)+(k'^2a, k'^2b)$ by definition.

$=[(k^2+k'^2)a, (k^2+k'^2)b]$ by def.

Also by given definition L.H S $=(k+k')(a, b)$

$=[(k+k')^2 a, (k+k')^2 b]$

Since $(k+k')^2 \neq k^2+k'^2$ $\therefore$ L.H.S. $\neq$ R.H.S.

Hence one of the laws of scalar multiplication is not satisfied. Hence V is not a vector space over R.

§ 3. Properties of vector space.

If V (F) be a vector space then

I. $a.0=0$ where $a \in F$ and 0 on both sides represents a vector $\in V$. **(Delhi 70; Meerut 69)**

We know that $a(\alpha+\beta)=a\alpha+a\beta \ \forall \ \alpha, \beta \in V$ and $a \in F$

Choosing $\beta=0$ we have

$$a(\alpha+0)=a\alpha+a0$$

or $$a\alpha=a\alpha+a0$$

or $$a\alpha+0=a\alpha+a0 \quad \text{or} \quad 0=a0$$

or $a0=0$ by cancellation law as $(V, +)$ is a group and cancellation law holds in a group.

II. $0\alpha=0$ where 0 on the left is a scalar and 0 on the right is a vector and $\alpha \in V$.

(Delhi 70; Meerut 69)

We know that $(a+b)\alpha=a\alpha+b\alpha$. Choosing $b=0$ scalar

$$(a+0)\alpha=a\alpha+0\alpha.$$

or $$a\alpha=a\alpha+0\alpha$$

or $$a\alpha+0=a\alpha+0\alpha$$

or $$0=0\alpha \text{ by Cancellation Law}$$

or $$0\alpha=0$$

III. $(-a)\alpha=-(a\alpha)$, $a \in F$ and $\alpha \in V$.

(Delhi 70; Meerut 69)

$$a\alpha+(-a)\alpha=[a+(-a)]\alpha=0\alpha=0 \qquad \text{by II}$$

$\because \ a\alpha+b\alpha=(a+b)\alpha$

$\therefore \ (-a)\alpha=-(a\alpha)$ and in particular $(-1)\alpha=-\alpha$.

IV. $a(-\alpha)=-(a\alpha)$

$a(-\alpha)+a\alpha=a[(-\alpha)+\alpha]=a\ 0=0$ by I

$\because \ a\alpha+a\beta=a(\alpha+\beta)$

$\therefore \ a(-\alpha)=-(a\alpha)$.

V. $a(\alpha-\beta)=a\alpha-a\beta$.

$a(\alpha-\beta)=a[\alpha+(-\beta)]=a\alpha+a(-\beta)$

$=a\alpha-a\beta$. by IV.

Ex. 1. *If $V(F)$ is a vector space then prove the following*

(i) $(-1)\alpha=-\alpha$.

(ii) $\beta+(\alpha-\beta)=\alpha$.

(iii) If $a\alpha=0$ then either $a=0$ or $\alpha=0$ where $\alpha, \beta \in V$ and $a \in F$.

(i) We know that

$(-a)\alpha=-(a\alpha)$. § 3.

Choosing $a=1$ we get

$(-1)\alpha=-(1.\alpha)=-\alpha$. $\because$ $1.\alpha=\alpha$.

(ii) $\{\beta+(\alpha-\beta)\}=\beta+\alpha+(-\beta)$

$=\beta+(-\beta)+\alpha$. Commutative prop.

$=0+\alpha=\alpha$

$\because$ 0 is the identity of $(V, +)$

(iii) Let $a\alpha=0$ and $a\neq 0$.

Then we should show that $\alpha=0$.

Since $a\neq 0$ and $a \in F$ in which all non zero elements are invertible $\therefore$ a^{-1} exists s.t. $a^{-1}a=a\,a^{-1}=1$.

Now $\alpha=1.\alpha=(a^{-1}a)\alpha=a^{-1}(a\alpha)=a^{-1}(0)=0$.

Again $a\alpha=0$ and let us suppose that $\alpha\neq 0$ then it would mean that $a=0$ because if $a\neq 0$ than as shown above $\alpha=0$ which will be a contradiction to our supposition $\alpha\neq 0$.

Ex. 2. *If $V(F)$ is a vector space then prove that each of the following cancellation laws hold good.*

(i) $a\alpha=b\alpha \Rightarrow a=b$; $\alpha\neq 0$, $a, b \in F$

(ii) $a\alpha=a\beta \Rightarrow \alpha=\beta$, $a\neq 0$, $\alpha, \beta \in F$.

(i) $a\alpha=b\alpha \Rightarrow a\alpha+(-b)\alpha=0 \Rightarrow (a+(-b))\alpha=0$

$\Rightarrow a+(-b)=0$ [by Ex 1] $\because$ $\alpha\neq 0$ given

$\Rightarrow a=b$.

(ii) Since $a \neq 0$ $\therefore$ a^{-1} exists s.t. $aa^{-1}=a^{-1}a=1$

$\therefore$ $a\alpha=a\beta \Rightarrow a^{-1}(a\alpha)=a^{-1}(a\beta)$

$\Rightarrow (a^{-1}a)\alpha=(a^{-1}a)\beta$ $\because$ $(ab)\alpha=a(b\alpha)$

$\Rightarrow 1.\alpha=1.\beta \Rightarrow \alpha=\beta$.

§ 4. Vector Sub space.

Definition *A non empty sub set W of a Vector space V over a field F is called a sub space of V if W is a vector space over F w.r.t. addition and scalar multiplication.*

(B.H.U. 70; Delhi Hon's. 70; Kanpur 69; Meerut 68)

§ 5. Criteria for a Sub space.

Theorem. I. *The necessary and sufficient condition for a non-empty sub-set W of a vector space V (F) to be a sub-space of V is that W is closed under vector addition and scalar multiplication.*

Necessary : Given W is a sub space. By definition W is a vector space for the two compositions of addition and scalar multiplication in V. Hence W should be closed for the two compositions.

Sufficient : Given W is closed both for addition and scalar multiplication. We will show that W is a vector space.

Let $1 \in F \Rightarrow -1 \in F$ by def, of F

Now $-1 \in F, \alpha \in W \Rightarrow -1.\alpha \in W \Rightarrow -\alpha \in W$

Thus inverse of each $\alpha \in W$ is in W.

Again $\alpha \in W, -\alpha \in W \Rightarrow \alpha+(-\alpha) \in W \Rightarrow 0 \in W$

Thus identity exists and belongs to W.

Addition in W is associative and commutative as it is so in V and W is a subset of V.

W is closed for addition as given

Hence W is an additive abelian group.

Further W is closed for scalar multiplication and laws of scalar multiplication hold good for W also as they hold good for V and W is a subset of V.

Thus W is a vector space for the two compositions and hence by definition it is a sub-space.

As an example, we know that the set of all ordered triads of real numbers is a vector space

i.e., $$V=\{(a_1, a_2, a_3) : a_i \in R.\}$$

with the usual definition of addition and scalar multiplication.

Now if we choose $W_1=\{(a_1, a_2, 0),\ a_1, a_2 \in R\}$.

i.e., the set of all vectors in $X\ 0\ Y$ plane then

$$(a_1, a_2, 0)+(b_1, b_2, 0)=(a_1+b_1, a_2+b_2, 0) \in W_1$$

and $$k\ (a_1, a_2, 0)=(ka_1, ka_2, 0) \in W_1.$$

i.e., W_1 is closed w.r.t., addition and scalar multiplication and as such W_1 is a sub space of V over R.

Similarly $W_2=(a_1, 0, 0)$, *i e.* the set of all vectors along x-axis is also a sub space of V over R.

Trivial Sub Spaces.

Again we know that the set V is a sub set of V and also the set $\{0\}$ is also a sub set of V. Both these are vector spaces for the two compositions of addition and scalar multiplication of $V\ (F)$. Hence both V and $\{0\}$ are spaces which are called trivial or improper sub spaces and all other sub spaces will be called non trivial or proper.

Theorem 2. *A non empty sub set W of a vector space $V\ (F)$ is a sub space of V if and only if*

(*i*) $\alpha \in W, \beta \in W \Rightarrow \alpha-\beta \in W$

(*ii*) $a \in F, \alpha \in W \Rightarrow a\alpha \in W$

Necessary : W is sub space given.

Since W is a sub space and hence it is an additive

abelian group rather an additive sub group of V and hence

$$\alpha \in W, \beta \in W \Rightarrow \alpha - \beta \in W.$$

Also W is closed for scalar multiplication as it is a sub-space. by Th. I

$$\therefore \quad a \in F, \alpha \in W \Rightarrow a\alpha \in W$$

Hence both the conditions 1 and 2 hold good.

Sufficient. The two given conditions hold good.

$\alpha \in W, \alpha \in W \Rightarrow \alpha - \alpha \in W \Rightarrow 0 \in W$

Again $0 \in W, \alpha \in W \Rightarrow 0 - \alpha \in W \Rightarrow -\alpha \in W$

Now $\alpha \in W, \beta \in W \Rightarrow \alpha \in W, -\beta \in W$

$$\Rightarrow \alpha - (-\beta) \in W \Rightarrow \alpha + \beta \in W$$

Thus W is closed for addition and by condition (2) W is closed for scalar multiplication. Hence by Th. I W is a sub space.

Theorem 3. *A sub set W of a vector space $V(F)$ is a sub space of V if and only if*

$$a, b \in F, \alpha, \beta \in V \Rightarrow a\alpha + b\beta \in W \qquad \textbf{(M. U. 69)}$$

Necessary. Let W be a sub space then W is closed both for addition and scalar multiplication.

$$a \in F, \alpha \in W \Rightarrow a\alpha \in W$$
$$b \in F, \beta \in W \Rightarrow b\beta \in W.$$

Now $a\alpha \in W, b\beta \in W \Rightarrow a\alpha + b\beta \in W$ by def. of sub space *i e.* W is closed for addition.

Sufficient. Given that

$$a, b \in F, \alpha, \beta \in V \Rightarrow a\alpha + b\beta \in W$$

To prove that W is a sub space

Choosing $a=1, b=1$ we get $1.\alpha + 1.\beta \in W$

or $\alpha + \beta \in W$, Hence W is closed for addition.

Again putting $b=0$, we get

$$a\alpha + 0\beta \in W \text{ or } a\alpha \in W \quad \because \quad 0\beta = \mathbf{0}.$$

Thus W is closed under scalar multiplication.

Hence by Th. 1 W is a sub space.

Note : We can modify the above criteria as $c \in F$, $\alpha, \beta \in W \Rightarrow c\alpha+\beta \in W$ then W is a sub space.

Intersection of two sub spaces

Theorem 4. *The intersection of any two sub spaces W_1 and W_2 of a vector space $V(F)$ is also a sub space.*

(B.H U. 70; Delhi 69; Meerut 70)

Let α, β be any two vectors $\in W_1 \cap W_2$ and a, b be any two scalars. In order to prove that $W_1 \cap W_2$ is a sub space we shall establish that $a\alpha+b\beta \in W_1 \cap W_2$ and hence by Theorem 3, $W_1 \cap W_2$ will be a sub space.

Given $\alpha \in W_1 \cap W_2 \Rightarrow \alpha \in W_1, \alpha \in W_2$

$\beta \in W_1 \cap W_2 \Rightarrow \beta \in W_1, \beta \in W_2$

Now $\alpha \in W_1, \beta \in W_1 \Rightarrow a\alpha+b\beta \in W_1$

by Theorem 3 as W_1 is a sub space.

Similarly $\alpha \in W_2, \beta \in W_2 \Rightarrow a\alpha+b\beta \in W_2$ as above

Since $a\alpha+b\beta \in W_1$ as well as $\in W_2$

$\therefore \quad a\alpha+b\beta \in W_1 \cap W_2$

Hence $W_1 \cap W_2$ is a sub space.

In general we can say that any intersection of a family of sub spaces is again a sub space.

As an illustration we know if

$$V(F)=R^3(R)=\{(x, y, z) : x, y, z \in R\}$$

then $W_1=\{(x, y, 0)\}$ and $W_2=\{(x, 0, z)\}$ are also sub spaces of $R^3(R)$ as shown on P. 299.

$W_1 \cap W_2=\{x, 0, 0\}$ is also a sub space of $R^3(R)$ which is the set of all vectors along x-axis.

$W_1 \cap W_2$ is the largest sub set contained both in W_1 and W_2 and hence $W_1 \cap W_2$ is the largest sub space contained in both W_1 and W_2.

Ex. 1. *Prove that the intersection of any family of sub spaces of a vector space is a sub space.* **(Meerut M.Sc. 68)**

Let $W_1, W_2, \ldots, W_n$ be sub spaces of a vector space $V(F)$ and $W = \cap W_i = \{\alpha \in V : \alpha \in W_i \ \forall\ i = 1, \ldots, n\}$.

Clearly W is non empty as $\mathbf{0} \in W_i \ \forall\ i$

and hence $\mathbf{0} \in \cap W_i$ *i.e.* W.

Let $a, b \in F$ and, $\alpha, \beta \in W$ then $\alpha, \beta \in$ each W_i

$\Rightarrow a\alpha + b\beta \in$ each W_i which is a sub space

$\Rightarrow a\alpha + b\beta \in \cap W_i \Rightarrow a\alpha + b\beta \in W$.

Hence $W = \cap W_i$ is a sub space.

Union of two sub spaces is not necessarily a sub space.

Let $V_3(F)$ be a vector space and W_1 and W_2 be its two sub spaces whose elements are of the type $(a, 0, 0)$, $(0, b, 0)$ respectively.

Choose $\alpha = (a_1, 0, 0) \in W_1$

$\beta = (0, b_1, 0) \in W_2$.

Now $x \in W_1 \cup W_2 \Rightarrow x \in W_1$ or $x \in W_2$

If $\alpha \in W_1 \cup W_2$ and $\beta \in W_1 \cup W_2$

then $a\alpha + b\beta = a(a_1, 0, 0) + b(0, b_1, 0)$

$= (aa_1, 0, 0) + (0, bb_1, 0)$

$= (aa_1, bb_1, 0)$

and this does not belong to either W_1 or W_2 and hence does not belong to $W_1 \cup W_2$.

Since $a\alpha + b\beta$ does not belong to $W_1 \cup W_2$ and as such by Theorem 3. $W_1 \cup W_2$ is not a sub space.

Ex. 2. *Prove that union of two sub spaces W_1 and W_2 is sub space if and only if one is contained in the other.*

1st Case. Let $W_1 \subset W_2$ then $W_1 \cup W_2 = W_2$

Since W_2 is sub space therefore $W_1 \cup W_2$ is also a sub space.

Similarly if $W_2 \subset W_1$ then $W_1 \cup W_2 = W_1$ and as W_1 is a sub space it follows that $W_1 \cup W_2$ is also a sub space,

2nd Case. Let $W_1 \cup W_2$ be a sub space and we shall prove that either $W_1 \subset W_2$ or $W_2 \subset W_1$.

Suppose W_1 is not a sub set of W_2 and W_2 is not a sub set of W_1.

Since $W_1 \not\subset W_2 \Rightarrow \exists\ \alpha \in W_1,\ \alpha \notin W_2$ ..(1)

$W_2 \not\subset W_1 \Rightarrow \exists\ \beta \in W_2,\ \beta \notin W_1$ ...(2)

Now from above relations we can say that

$\alpha \in W_1 \cup W_2$ [as $\alpha \in W_1$],

$\beta \in W_1 \cup W_2$ [as $\beta \in W_2$].

But $W_1 \cup W_2$ is a sub space and hence

$\alpha+\beta$ also $\in W_1 \cup W_2$.

Since $\alpha+\beta \in W_1 \cup W_2$ it follows that

$\alpha+\beta \in W_1$ or W_2

Let $\alpha+\beta \in W_1$, also $\alpha \in W_1$ and W_1 is a sub space

$\therefore\ (\alpha+\beta)-\alpha \in W_1$ or $\beta \in W_1$.

But from (2) $\beta \notin W_1$ and hence a contradiction

Therefore either $W_1 \subset W_2$ or $W_2 \subset W_1$

§ 6. Linear sum of two sub spaces.

Definition. *If W_1 and W_2 be two sub spaces of the vector space $V(F)$ then the linear sum of these two sub spaces denoted by W_1+W_2 is the totality of elements obtained on adding each element of W_1 to each element of W_2. In other words it is the set of all sums $\alpha_1+\alpha_2$ such that $\alpha_1 \in W_1$ and $\alpha_2 \in W_2$.*

or $W_1+W_2=\{\alpha_1+\alpha_2 : \alpha_1 \in W_1$ and $\alpha_2 \in W_2\}$

Let $\alpha_1 \in W_1$ and $0 \in W_2$

Now $\alpha_1 \in W_1 = \alpha_1+0 \in W_1+W_2$ $\therefore$ $W_1 \subset W_1+W_2$

Similarly $0 \in W_1$ and $\alpha_2 \in W_2$

Now $\alpha_2 \in W_2 = 0+\alpha_2 \in W_1+W_2$ $\therefore$ $W_2 \subset W_1+W_2$

Theorem 5. *If W_1 and W_2 be two sub spaces of $V(F)$ then* **(Meerut B.Sc. 70)**

W_1+W_2 is a sub space of $V(F)$

Let $\alpha_1, \beta_1 \in W_1$ and $\alpha_2, \beta_2 \in W_2$
so that $\alpha=\alpha_1+\alpha_2 \in W_1+W_2$ and $\beta=\beta_1+\beta_2 \in W_1+W_2$.

In order to prove that W_1+W_2 is a sub space we have to establish

$a\alpha+b\beta \in W_1+W_2$ where $\alpha, \beta \in W_1+W_2$.

Now $a\alpha+b\beta=a(\alpha_1+\alpha_2)+b(\beta_1+\beta_2)$
$=(a\alpha_1+b\beta_1)+(a\alpha_2+b\beta_2) \in W_1+W_2$, $a, b \in F$

Because $\alpha_1, \beta_1 \in W_1$
$\therefore$ $a\alpha_1+b\beta_1 \in W_1$ as W_1 is a sub space
$\alpha_2, \beta_2 \in W_2$ $\therefore$ $a\alpha_2+b\beta_2 \in W_2$ as W_2 is a sub space

Hence W_1+W_2 is a sub space.

§ 7. Direct sum of two sub spaces.

If W_1 and W_2 be two sub spaces of a vector space $V(F)$ then if $V=W_1+W_2$ *i.e.* V is the linear sum of two sub spaces W_1 and W_2 then as explained in § 6 it means that an

$$Z \in V=\alpha+\beta$$

for some $\alpha \in W_1$ and some $\beta \in W_2$.

But if $Z \in V=\alpha+\beta$ for a **unique** $\alpha \in W_1$ and a **unique** $\beta \in W_2$ then in this case $V=W_1+W_2$ *i.e.* linear sum al right but because of unique representation of Z it will be termed as "**V is the direct sum of its two subspaces W_1 and W_2.** and is expressed as $V=W_1 \oplus W_2$.

The following examples will make clear the distinction between the linear sum and direct sum of two spaces

Ex. 1. *$V_3(R)$ is a vector space and any vector $Z \in V$*

$$=(a, b, c)$$

Also we know that

$W_1=\{a, b, 0) : a, b \in R\}$ is a subspace of V_3

$W_2=\{(0, 0, c) : c \in R\}$ is a sub space of V_3

Now $(a, b, c)=(a, b, 0)+(0, 0, c)$ or $Z=\alpha+\beta$ ...(1)

where $Z \in V$ and $\alpha \in W_1$, $\beta \in W_2$

$\therefore$ $V_3(R)=W_1+W_2$ al-right.

Again there cannot be any other way of writing the result (1) *i.e.* there cannot be any other element of W_1 and any other element of W_2 such that their sum is Z *i.e.* (a, b, c) in V. In other words the representation (1) is unique and hence instead of calling V as the linear sum of sub spaces W_1 and W_2 *i.e.* $V=W_1+W_2$ we shall say that V is the direct sum of sub spaces W_1 and W_2 *i.e.* $V=W_1 \oplus W_2$.

2. *$V_3(R)$ is a vector space and any vector*

$Z \in V=(a, b, c)$.

Also $W_1=\{(a, 0, c) : a, b \in R\}$ is a sub space of V_3.

$W_2=\{(0, b, c) : b, c \in R\}$ is a sub space of V_3.

$$Z \in V=(a, b, c)=\left(a, 0, \frac{c}{2}\right)+\left(0, b, \frac{c}{2}\right)$$

$$=\left(a, 0, \frac{c}{4}\right)+\left(0, b, \frac{3c}{4}\right)$$

i.e. $Z=\alpha_1+\beta_1=\alpha_2+\beta_2$. with $\alpha_1, \alpha_2 \in W_1$, $\beta_1, \beta_2 \in W_2$.

Above shows that the representation is not unique and so in this case

$V=W_1+W_2$ only and $V \neq W_1 \oplus W_2$

i.e. V is the linear sum of two sub spaces and not their direct sum.

Now we are in a position to define the direct sum as under.

Definition. *A vector space V (F) is said to be direct sum of its two sub spaces W_1 and W_2 if for every element*

$Z \in V$ there exists a unique element $\alpha \in W_1$ and a unique element $\beta \in W_2$ such that $Z=\alpha+\beta$.

and in this case $V=W_1 \oplus W_2$.

Theorem 6. Criteria for direct sum.

If a vector space $V(F)$ be the linear sum of its two sub spuces W_1 and W_2 i.e. $V=W_1+W_2$ then

$$V=W_1 \oplus W_2 \Leftrightarrow W_1 \cap W_2=\{0\}. \quad \textbf{(Marthwada 70)}$$

Ist case Given $V=W_1 \oplus W_2$. **To prove** $W_1 \cap W_2=\{0\}$.

If possible let a non zero vector $Z \in W_1 \cap W_2$

$\therefore$ $Z \in W_1$ and $Z \in W_2$. Also $W_1 \cap W_2$ is a sub space of V.

$\therefore$ $Z \in W_1 \cap W_2 \Rightarrow Z \in V$.

Now $Z=0+Z$ with $0 \in W_1$ and $Z \in W_2$

$\in V$

$=Z+0$ with $Z \in W_1$ and $0 \in W_2$

Above relation shows that a non zero vector $Z \in V$ is expressible in at least two ways as the sum of a vector in W_1 and a vector in W_2 *i.e.* the representation is not unique and hence it contradicts that $V=W_1 \oplus W_2$. Therefore no non zero vector Z can belong to $W_1 \cap W_2$. Hence the only vector in $W_1 \cap W_2$ should be zero vector as $W_1 \cap W_2$ is a subspace.

$\therefore$ $V=W_1 \oplus W_2 \Rightarrow W_1 \cap W_2=\{0\}$.

2nd case. Given $W_1 \cap W_2=\{0\}$ and $V=W_1+W_2$

The prove. $V=W_1 \oplus W_2$

Since $V=W_1+W_2$ $\therefore$ $Z=\alpha+\beta$

$\in V$ $\in W_1$ $\in W_2$

We have only to show that the above representation is unique.

Let if possible there be another representation of Z as above *i.e.*

$$\left.\begin{aligned} Z&=\alpha+\beta \\ Z&=\alpha_1+\beta_1 \end{aligned}\right\} \alpha, \alpha_1 \in W_1 \text{ and } \beta, \beta_1 \in W_2$$

$\therefore \quad \alpha+\beta=\alpha_1+\beta_1 \Rightarrow \alpha-\alpha_1=\beta_1-\beta$

But $\alpha, \alpha_1 \in W_1 \Rightarrow \alpha-\alpha_1 \in W_1$ as W_1 is a subspace

Also $\beta, \beta_1 \in W_2 \Rightarrow \beta_1-\beta \in W_2$ as W_2 is a subspace

Since $\alpha-\alpha_1=\beta_1-\beta$ we conclude that an element of W_1 is same as an element of W_2 *i.e.* W_1 and W_2 have common element.

But $W_1 \cap W_2=\{0\}$ given and hence $\alpha-\alpha_1$ and $\beta_1-\beta$ both should be zero vector

$$\therefore \quad \alpha-\alpha_1=0 \text{ and } \beta_1-\beta=0$$

or $\alpha_1=\alpha$ and $\beta_1=\beta$

This establishes that the representation $Z=\alpha+\beta$ is unique and hence

$V=W_1 \oplus W_2$, by def of direct sum.

Disjoint subspaces. *Two sub spaces W_1 and W_2 are said to be disjoint if and only if their intersection is a zero subspace i.e. $W_1 \cap W_2=\{0\}$.*

Complementary subspaces.

If $V=W_1 \oplus W_2$, then the two subspaces W_1 and W_2 are said to be complementary subspaces.

Extension of the defi. ition of direct sum.

A vector space $V(F)$ is said to be direct sum of its sub spaces $W_1, W_2 \ldots W_n$

i.e. $V=W_1 \oplus W_2 \ldots\ldots \oplus W_n$, if and only if a vector $Z \in V$ is uniquely expressible as

$$Z=\alpha_1+\alpha_2 \ldots\ldots \alpha_n. \text{ with } \alpha_i \in W_i$$

Complementary subspaces are not unique.

Consider the vector space $V_3(R)$ then the following are its subspaces

$M_1=\{(0, a_2, a_3)\}$ yz plane $\quad N_1=\{(a_1, 0, 0)\}$ x axis
$M_2=\{(a_1, 0, a_3)\}$ zx plane $\quad N_2=\{0, a_2, 0\}$ y axis
$M_3=\{a_1, a_2, 0\}$ xy plane $\quad N_3=\{0, 0, a_3\}$ z axis

then we can write

$$V=M_1\oplus N_1=M_2\oplus N_2=M_3\oplus N_3=N_1\oplus N_2\oplus N_3.$$

Above shows that complementary subspaces of a vector space are not unique.

Corresponding to a given sub space there will be a unique complementary sub space.

Let W_1 be a given sub space and W_2 and W_3 be its complementary sub spaces so that $V=W_1\oplus W_2$ and $V=W_1\oplus W_3$

or $\quad Z=\alpha_1+\alpha_2 \qquad \alpha_1\in W_1, \alpha_2\in W_2$
and $\quad Z=\alpha_1+\alpha_3 \qquad \alpha_1\in W_1, \alpha_3\in W_3$

$\therefore \quad \alpha_1+\alpha_2=\alpha_1+\alpha_3$

$\therefore \quad \alpha_2=\alpha_3$ by left concellation law.

$\therefore \quad W_2=W_3$. Hence we have a unique complementary sub space W_2 corresponding to given sub space W_1 such that

$$V=W_1\oplus W_2$$

Excercise 2

Ex. 1. *Let* $V=R^3=\{x, y, z) : x, y, z \in R\}$ *and if* W *be the set of all triplets* (x, y, z) *such that (i)* $x-3y+4z=0$ *(ii)* $a_1x+b_1y+c_1z=0$ *then prove that* W *is a sub space of* R^3 (R).

Let $\quad \alpha=(x_1, y_1, z_1)\in W$

$\qquad \beta=(x_2, y_2, z_2)\in W$

$\therefore \quad x_1-3y_1+4z_1=0 \qquad x_2-3y_2+4z_2=0 \qquad \ldots(A)$

Now $\quad a\alpha+b\beta=(ax_1+bx_2, ay_1+by_2, az_1+bz_2)$ by def.

If will belong to W if we show that

$$(ax_1+bx_2)-3(ay_1+by_2)+4\ (az_1+bz_2)=0$$

or $a(x_1-3y_1+4z_1)+b(x_2-3y_2+4z_2)=0$

$a.0+b.0=0$ by (A)

Hence $a\alpha+b\beta \in W$. which therefore is a subspace Similarly we can prove the second part.

Ex. 2. *Find out whether the following are sub spaces of* R^4 (R) *where* $R^4=\{(x, y, z, w) : x, y, z, w \in R\}$.

(a) $W=\{(x, x, x, x)\} : x \in R\}$.

Let α, β be any two elements of W and $a, b \in F$ *i.e.* R then

$$a\alpha+b\beta=a\,(x, x, x, x)+b\,(y, y, y, y) : x, y \in R$$
$$=(ax, ax, ax, ax)+(by, by, by, by)$$
$$=(ax+by, ax+by, ax+by, ax+by)$$
$$=(A, A, A, A) \in W$$

$\because$ $A=ax+by \in R$ as $a, b, x, y \in R$.

Hence W is a sub space.

(b) $W=\{(x, y, x, y) : x, y \in I)$.

Let $\alpha=(x, y, x, y)$, $\beta=(u, v, u, v)$ and $a, b \in F$ *i.e.* R and $x, y, u, v \in I$

then $a\alpha+b\beta=a\,(x, y, x, y)+b\,(u, v, u, v)$
$$=(ax, ay, ax, ay)+(bu, bv, bu, bv)$$
$$=(ax+bu, ay+bv, ax+bu, ay+bv)$$
$$=(A, B, A, B).$$

But $A=ax+bu$ may not be an integer when x, u are integers but $a, b \in R$ *e.g.* if $x=2$, $u=3$ and $a=\frac{1}{7}$, $b=\frac{8}{3}$ then $ax+bu=\frac{1}{7}.2+\frac{8}{3}.3=\frac{170}{7}$ which is not an integer.

Hence $a\alpha+b\beta \notin W$ and as such W is not a sub space.

(c) $W=\{(x, 2x, y, x+y) : x, y \in R\}$

Let $\alpha=(x, 2x, y, x+y)$, $\beta=(u, 2u, v, u+v)$ where $x, y, u, v \in R$ and suppose $a, b \in F$ *i.e.* R then $a\alpha+b\beta=a\,(x, 2x, y, x+y)+b\,(u, 2u, v, u+v)$

$$=\{(ax, 2ax, ay, a(x+y)\}+\{(bu, 2bu, bv, b(u+v)\}$$
$$=\{ax+bu, 2(ax+bu), (ay+bv),$$
$$(ax+bu+ay+bv)\}$$
$$=(A, 2A, B, A+B)$$

where both A and $B \in R$ as $a, b, x, y, u, v \in R$

$\therefore$ $a\alpha+b\beta \in W$ which therefore is a sub space.

Ex. 3. *If a vector space is the set of real valued continuous functions over R, then show that the set W of solutions of differential equation* $2\frac{d^2y}{dx^2}-9\frac{dy}{dx}+2y=0$ *is a sub space of V.*

$$W=\left\{ y : 2\frac{d^2y}{dx^2}-9\frac{dy}{dx}+2y=0 \right\} \text{ where } y=f(x).$$

Clearly $y=0$ satisfies the differential equation and as such it belongs to W. Now choose $y_1, y_2 \in W$.

$$\therefore\ 2\frac{d^2y_1}{dx^2}-9\frac{dy_1}{dx}+2y_1=0$$
$$2\frac{d^2y_2}{dx^2}-9\frac{dy_2}{dx}+2y_2=0.$$

If W is to be a sub space then we should show that ay_1+by_2 also belongs to W where $a, b \in F$

or $$2\frac{d^2}{dx^2}(ay_1+by_2)-9\frac{d}{dx}(ay_1+by_2)+2(ay_1+by_2)=0$$

or $$2a\frac{d^2y_1}{dx^2}+2b\frac{d^2y_2}{dx^2}-9\left(a\frac{dy_1}{dx}+b\frac{dy_2}{dx}\right)+2ay_1+2by_2=0$$

or $$a\left(2\frac{d^2y_1}{dx^2}-9\frac{dy_1}{dx}+2y_1\right)$$
$$+b\left(2\frac{d^2y_2}{dx^2}-9\frac{dy_2}{dx}+2y_2\right)=0$$

or $a.0+b.0=0$. Hence true.

Since ay_1+by_2 satisfies the given differential equation as and when y_1 and y_2 satisfy it therefore W is a sub space.

Ex. 4. *Show that the set of all polynomials in one indeterminate x over a field F of degree less than or equal to n is a sub space of the vector space of all polynomials over F*

$P(x)=\{p(x) : p(x)=a_0+a_1x+a_2x^2+\ldots\ldots\}$, $a_i \in F$.

We know that $P(x)$ is a vector space.

Let $W=\{p(x) : p(x)=a_0+a_1x+\ldots\ldots+a_nx^n\}$ $a_i \in F$ *i.e.* W is the set of all polynomials of degree less than or equal to n.

Evidently $W \subset P(x)$ and let

$$p_1(x)=\sum_{i=0}^{n} a_i x^i, \quad p_2(x)=\sum_{i=0}^{n} b_i y^i \in W$$

then $ap_1(x)+bp_2(x)$, where $a, b, \in F$

$$=a \Sigma a_ix^i+b \Sigma b_ix^i$$
$$=\Sigma (a\, a_i) x^i+\Sigma (h\, b_i) x^i$$
$$=\Sigma (a\, a_i+b\, b_i) x^i.$$

Since R. H. S. is again a polynomial of degree less than or equal to n and as such it belongs to W.

Therefore W is a sub space.

Ex. 5. *If V (C) is a vector space consisting of polynomials in x with complex coefficients, then prove the following*

(a) The set W_1 and W_2 of even and odd polynomials in x are sub spaces.

(b) W_1 and W_2 are complementary sub spaces.

$V(C)=\{p(x) : p(x)=a_0+a_1x+a_2x^2+\ldots.\}$ $a_i \in C$.

$p(x)$ is said to be even if $p(-x)=p(x)$.

$p(x)$ is said to be odd if $p(-x)=-p(x)$.

$W_1=\{p(x) : p(x)$ is even polynomial$\}$

$\therefore \quad p(x)=a_0+a_2x^2+a_4x^4+\ldots\ldots$

Let $p(x)$ and $p'(x) \in W_1$ and $a, a' \in C$ then

$a.p(x)+a'.p'(x)$

$=a(a_0+a_2x^2+a_4x^4+\ldots)+a'(a_0'+a_2'x^2+a_4'x^4+\ldots)$

$=(a\,a_0+a'\,a'_0)+(a\,a_2+a'\,a'_2)\,x^2+(a\,a_4+a'\,a_4')\,x^4+\ldots$

Above is again an even polynomial and as such belongs to W_1 which therefore is a sub space. Each of the coefficient in the above $\in C$ as C is a field.

Similarly we can prove that the set W_2 of odd polynomials is a sub space.

i..e $\quad W_2=\{p(x) : p(x)$ is odd polynomial$\}$

i.e $\quad p(x)=a_1x+a_3x^3+a_5x^5+\ldots\ldots$

In order to slow that W_1 and W_2 are complementary we have to prove that

$V=W_1+W_2$ and $W_1 \cap W_2=\{0\}$ so that $V=W_1 \oplus W_2$ and W_1 and W_2 will in that case be complementary.

$Z \in V=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4+\ldots\ldots$

$=(a_0+a_2x^2+a_4x^4+\ldots)+(a_1x+a_3x^3+\ldots)$

$=$poly in W_1+poly in W_2.

$\therefore \quad V=W_1+W_2$.

Secondly let $p(x) \in W_1 \cap W_2 \Rightarrow p(x) \in W_1$ and W_2.

$\therefore \quad p(-x)=p(x) \quad$ as $\quad p(x) \in W_1$

$p(-x)=-p(x) \quad$ as $\quad p(x) \in W_2$,

$\therefore \quad p(x)=-p(x) \quad$ or $\quad 2p(x)=0$

or $\quad p(x)=0 \quad$ *i.e.* zero polynomial.

$\therefore \quad W_1 \cap W_2=\{0\}$.

$\therefore \quad V=W_1 \oplus W_2$ and therefore W_1 and W_2 are complementary sub spaces of V.

Ex. 6. *Let $V(R)$ be a vector space of all functions from R into R and W_1 and W_2 be the sub sets containing even and odd functions respectively then prove that*

(*a*) *W_1 and W_2 are sub spaces of $V(R)$.*

(*b*) *W_1 and W_2 are complementary sub spaces.*

A function f is said to be even if $f(-x)=f(x)$ and odd if

$$f(-x)=-f(x).$$

Proceed as in Ex. 5.

§ 8. Linear Combination of Vectors.

Definition. *If $V(F)$ be a vector space and $\alpha_1\ \alpha_2\ .\ \alpha_n \in V$ and $a_1, a_2 \ldots a_n \in F$ then the vector*

$$\alpha=a_1\alpha_1+a_2\alpha_2\ ..+a_n\alpha_n=\sum_{i=1}^{n} a_i\alpha_i \text{ is called linear}$$

combination of vectors $\alpha_1, \alpha_2 \ldots \alpha_n$.

However if we choose different set of scalars say $b_1, b_2\ \ b_n$ then we shall get another linear combination. Hence for a given set of vectors we will have various linear combinations.

It may be noted that the vector α such that $\alpha=\sum_{i}^{n} a_i\ \alpha_i$ is again a vector in V as $V(F)$ is closed both for addition and scalar mnltiplication.

Illustration.

Let us consider the vector space $V_3(R)$ and let

$$\alpha_1=(1, 1, 1),\ \alpha_2=(1, 2, 3),\ \alpha_3=(2, -1, 1).$$

We want to express a vector $\alpha=(1, -2, 5)$ as a linear combination of the given set of vectors $\alpha_1, \alpha_2, \alpha_3$.

Let $\alpha=a_1\alpha_1+a_2\alpha_2+a_3\alpha_3\ \ a_i \in R$

$$\therefore\ (1, -2, 5)=a_1\ (1, 1, 1)+a_2\ (1, 2, 3)+a_3\ (2, -1, 1)$$
$$=(a_1, a_1, a_1)+(a_2, 2a_2, 3a_2)+(2a_3, -a_3, a_3)$$
$$=(a_1+a_2+2a_3,\ a_1+2a_2-a_3,\ a_1+3a_2+a_3)$$

By coordinate wise addition.

$\therefore$ $a_1+a_2+2a_3=1$ Eliminating a_1 we get

$a_1+2a_3-a_3=-2$ $a_2-3a_3=-3$

$a_1+3a_2+a_3=5$ $a_2+2a_3=7.$

Solving we get $5a_3=10$ $\therefore$ $a_3=2$; $a_2=3$

and hence $a_1=-6.$

$$\alpha=-6\alpha_1+3\alpha_2+2\alpha_3$$

and as such α is a 1. c. of $\alpha_1, \alpha_2, \alpha_3$

Similarly we can wirte

$$\alpha=-3\alpha_1+2\alpha_2.$$

where $\alpha=(1, 7, -4)$, $\alpha_1=(1, -3, 2)$ and $\alpha_2=(2, -1, 1)$ in $V_3(R)$.

But a vector $\alpha=(2, -5, 4)$ can not be expressed as a 1. c. of vectors $\alpha_1=(1, -3, 2)$ and $\alpha_2=(2, -1, 1)$ in $V_3(R)$ as in this case the equations giving the values of a_1, a_2 will be inconsistent.

§ 9. Linear span of a set.

Def. *The linear span of a non empty sub set S of a $V(F)$ is the set of all linear combinations of any finite number of elements of S and is denoted by $L(S)$.*

In other words.

$$L(S)=\{a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n : \alpha_i \in S \text{ and } a_i \in F \quad i=1, 2, \ldots n\}.$$

Theorem 7. *The linear span $L(S)$ of any sub set S of V is a sub space of V.*

Let α, β be any two elements of $L(S)$ then by definition of $L(S)$.

$$\alpha=a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n$$

$$\beta=b_1\beta_1+b_2\beta_2+\ldots+b_m\beta_m$$

where $\alpha_i \in S$ and $a_i \in F$, $i=1$ to n,

$\beta_j \in S$ and $b_j \in F$, $j=1$ to m.

In order to prove that $L(S)$ is a sub space we have to establish that for

$a, b \in F$ and $\alpha, \beta \in L(S)$, $a\alpha+b\beta \in L(S)$. (Th. 3 P. 300)

$$a\alpha+b\beta=a\sum_{i=1}^{n} a_i\alpha_i+b\sum_{j=1}^{m} b_j\beta_j$$

$$=\sum_{i=1}^{n}(aa_i)\ \alpha_i+\sum_{j=1}^{m}(bb_j)\ \beta_j$$

$$=\sum_{i=1}^{n} A_i\alpha_i+\sum_{j=1}^{m} B_j\beta_j$$

Above shows that $a\alpha+b\beta$ can be expressed as a linear combination of the vectors $\alpha_1, \alpha_2, \ldots \alpha_n, \beta_1, \beta_2, \ldots \beta_m$ belonging to S and as such it should belong to $L(S)$.

Hence $a\alpha+b\beta \in L(S)$ when $a, b \in F$ and $\alpha, \beta \in L(S)$ proving thereby that $L(S)$ is a sub space.

As an example, let us consider the set

$$S=\{(1, 0, 0), (0, 1, 0)\}$$

i.e. S is a sub set of $V_3(R)$ consiting of unit vectors along x axis and y axis.

$$L(S)=\{\alpha : \alpha \text{ is } a.\ L.\ C. \text{ of elements of } S\}$$

$$\therefore \quad \alpha=a_1(1, 0, 0)+a_2(0, 1, 0),\ a_1, a_2 \in F$$

$$=(a_1, 0, 0)+(0, a_2, 0)=(a_1, a_2, 0).$$

$$\therefore\ L(S)=\{\alpha : \alpha=(a_1, a_2, 0) \textit{ i.e. } XOY \text{ plane}\}$$

or $L(S)=W$ where W is the set of all points in XOY plane which we know is a sub space of $V_3(R)$

Theorem 8. *If S and T are sub sets of a vector space $V(F)$ then prove that*

(1) $S \subset L(T) \Rightarrow L(S) \subset L(T)$

(2) $S \subset T \Rightarrow L(S) \subset L(T)$

(3) *S is a sub space of V* $\Leftrightarrow L(S)=S$

(4) $L(L(S))=L(S)$

(5) $L(S \cup T)=L(S)+L(T)$

Proof. Given $S \subset L(T)$

To prove.. $L(S) \subset L(T)$

(1) Let $\alpha_i^s \in S$ and $a_i^s \in F$ and because $S \subset L(T)$

$\therefore \quad \alpha_i^s \in L(T)$. ...(1)

Now let $\alpha \in L(S) \Rightarrow \alpha = \sum_{i=1}^{n} a_i \alpha_i$ ...(2)

Since from (1) each $\alpha_i \in L(T)$ which is a sub-space,

$\therefore \quad \Sigma a_i \alpha_i$ also belong to $L(T)$

$\therefore \quad$ From (2), $\alpha \in L(T)$

Since $\alpha \in L(S) \Rightarrow \alpha \in L(T)$

$\therefore \quad L(S) \subset L(T)$.

(2) Given. $S \subset T$

To prove. $L(S) \subset L(T)$

Let $\alpha \in L(S)$. $\therefore \quad \alpha = \Sigma a_i \alpha_i$ ...(1)

But each $\alpha_i \in S \Rightarrow \alpha_i \in T \because S \subset T$

$\therefore \quad \Sigma a_i \alpha_i \in L(T)$

$\therefore \quad \alpha = \Sigma a_i \alpha_i \in L(T)$

Hence $\alpha \in L(S) \Rightarrow \alpha \in L(T) \quad \therefore L(S) \subset L(T)$

(3) **Given.** S is a sub space of V. To prove $L(S) = S$

Let $\alpha \in L(S) \Rightarrow \alpha = \Sigma a_i \alpha_i \Rightarrow \alpha' \in S$

because S is a sub space given and hence it is closed both for addition and scalar multiplication. $\therefore \quad L(S) \subset S$.

Also we know $S \subset L(S)$ as any vector $\alpha_i \in S$ can be written as a l. c. of all the vectors in S with scalars as zeros except 1 for the scalar coefficient of α_i.

Since $L(S) \subset S$ and $S \subset L(S) \quad \therefore L(S) = S$

Conversely. Given $L(S) = S$. **To prove** S is a sub space.

Since $L(S) = S$ and also we know that $L(S)$ is a sub space and hecne it follows that S is also a sub space.

(4) To prove. $L(L(S))=L(S)$.

Let us put $L(S)=T$ then since $L(S)$ is a sub space.

$\therefore$ T is a sub space and we have to prove that $L(T)=T$ when T is a sub space which is true by (3).

5. To prove $L(S \cup T)=L(S)+L(T)$

Let $\alpha \in L(S \cup T) \Rightarrow \alpha=\Sigma a_i\alpha_i$

Where $\alpha_i' \in S \cup T \Rightarrow$ some $x_i' \in S$ & some $\alpha_i' \in T$ and some α_i' may belong to both S and T. Restricting the common vectors to either S or T we can divide the vectors α_i' into α_j' and α_k' such that $\alpha_j' \in S$ and $\alpha_k' \in T$,

$\therefore$ $\alpha=\Sigma a_i x_i=\Sigma a_j\alpha_j+\Sigma a_k\alpha_k \Rightarrow \alpha \in L(S)+L(T)$

$\therefore$ $\alpha \in L(S \cup T) \Rightarrow \alpha \in L(S)+L(T)$

$\therefore$ $L(S \cup T) \subset L(S)+L(T)$. .. (1)

Now let $Z \in L(S)+L(T) \Rightarrow Z=x+y$

$\therefore$ $x \in L(S)$, $y \in L(T)$.

$\Rightarrow Z=\Sigma a_j x_j+\Sigma a_k x_k$, where $\alpha_j' \in S$ and $\gamma_k' \in T$.

$\Rightarrow Z=\Sigma a_i\alpha_i$ where $\{x_i\}=\{x_j\} \cup \{x_k\}$

$\Rightarrow Z \in L(S \cup T)$.

$\therefore$ $L(S)+L(T) \subset L(S \cup T)$ ...(2)

Hence from *1* and 2 we get $L(S \cup T)=L(S)+L(T)$

Excercise 3

Ex. 1 *Write the vector* $\alpha=(2, -5, 3) \in V$, *as a linear combination of the vectors* $\alpha_1=(1, -3, 2)$. $\alpha_2=(2, -4, -1)$, $\alpha_3=(1, -5, 7)$

Let $\alpha=a_1\alpha_1+a_2\alpha_2+a_3\alpha_3$ where $a_i' \in F$

$\therefore$ $(2, -5, 3)=a_1(1, -3, 2)+a_2(2, -4, -1)+a_3(1, -5, 7)$

or $(2, -5, 3)=(a_1+2a_2+a_3, -3a_1-4a_2-5a_3, 2a_1-a_2+7a_3)$

$\therefore$

$$\left.\begin{aligned} a_1+2a_2+a_3&=2 \\ -3a_1-4a_2-5a_3&=-5 \\ 2a_1-a_2+7a_3&=3 \end{aligned}\right\}$$

...(1) ...(2) ...(3)

Multiply first by 3 and add to second. Similarly multiply (1) by 2 and subtract from (3).

$$\therefore \quad 2a_2-2a_3=1 \quad \text{or} \quad a_2-a_3=1/2 \qquad \ldots(4)$$

$$\text{and} \quad -5a_2+5a_3=-1$$

$$\text{or} \quad a_2-a_3=\frac{1}{-} \qquad \ldots(5)$$

The above equations are clearly inconsistent as $a_2-a_3=1/2$ and also $1/5$.

Hence the given vector can not be expressed as a.l.c of the given vectors $\alpha_1, \alpha_2, \alpha_3$.

Ex. 2. *In the vector space* R^3 (R), *let*

$$\alpha=(1, 2, 1).\ \beta=(3, 1, 5).\ \gamma=(3, -4, 7),$$

prove that the sub spaces spanned by

$$S=\{\alpha, \beta\} \text{ and } T=\{\alpha, \beta, \gamma\} \text{ are the same.}$$

L (T) the linear span of T is a set of vectors which is a linear combination of vectors in T.

$$\therefore \quad L(T)=\{a\alpha+b\beta+c\gamma : a, b, c \in R\}$$

$$=a(1, 2, 1)+b(3, 1, 5)+c(3, -4, 7). \quad \ldots(1)$$

Let $(3, -4, 7)=x(1, 2, 1)+y(3, 1, 5)$.

$$\therefore \quad x+3y=3,\ 2x+y=-4,\ x+5y=7.$$

$\therefore$ $x=-3$, $y=2$ and these satisfy the 3rd relation also.

$$\therefore \quad (3, -4, 7)=-3(1, 2, 1)+2(3, 1, 5).$$

$$\therefore \quad c(3, -4, 7)=-3c(1, 2, 1)+2c(3, 1, 5).$$

$$\therefore \quad L(T)=a(1, 2, 1)+b(3, 1, 5)-3c(1, 2, 1)$$

$$+2c(3, 1, 5)$$

$$=(a-3c)(1, 2, 1)+(b+2c)(3, 1, 5)$$

$$=a'(1, 2, 1)+b'(3, 1, 5) \text{ where } a', b' \in R$$

$$=a'\alpha+b'\beta=L(S) \text{ by definition.}$$

Ex. 3. *If* $\alpha=(1, 2, -1)$, $\beta=(2, -3, 2)$, $\gamma=(4, 1, 3)$ *and* $\delta=(-3, 1, 2)$ *be the vectors in* R^3 (R), *show that*

$$L(\alpha, \beta) \neq L(\gamma, \delta).$$

Let us suppose that $L(\{\alpha, \beta\}) = L(\{\gamma, \delta\})$.

It would mean that there exists scalars $x, y \in R$ for **arbitrary** $a, b \in R$ such.

$$x\alpha + y\beta = a\gamma + b\delta$$

or $x(1, 2, -1) + y(2, -3, 2) = a(4, 1, 3) + b(-3, 1, 2)$

$$\Rightarrow (x+2y, 2x-3y, -x+2y) = (4a-3b, a+b, 3a+2b)$$

$$\Rightarrow x+2y = 4a-3b, \quad \ldots(1)$$

$$2x-3y = a+b, \quad \ldots(2)$$

$$-x+2y = 3a+2b. \quad \ldots(3)$$

Solving (1) and (3) for x and y, we get

$$x = \tfrac{1}{2}(a-5b) \text{ and } y = \tfrac{1}{4}(7a-b).$$

These should satisfy (2) also, *i.e.* $2x-3y = a+b$.

But $2x-3y = 2.\tfrac{1}{2}(a-5b) - 3.\tfrac{1}{4}(7a-b)$

$$= (1-2\tfrac{1}{4})a - (5-\tfrac{3}{4})b \neq a+b.$$

Hence (2) is not satisfied.

$$\therefore \quad L(\{\alpha, \beta\}) \neq L(\{\gamma, \delta\}).$$

It is however quite possible that there may be values of x, y for some particular values of a, b, as for example if we choose $a=1, b=-1$, then

$$x+2y=7, \quad 2x-3y=0, \quad -x+2y=1$$

and all these hold good for $x=3, y=2$.

But this would not mean that the sub space spanned by $\{\alpha, \beta\}$ and $\{\gamma, \delta\}$ are the same. For this there should exist $x, y \in R$ for **arbitrary** $a, b \in R$ such that

$$x\alpha + y\beta = a\gamma + b\delta$$

or satisfying equations 1, 2 and 3,

§ 10. Linear Dependence.

Definition. *A finite set* $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ *of vectors of a vector space* $V(F)$ *is said to be linearly dependent* (*L. D.*) *if*

there exists a set of scalars $a_1, a_2 \ldots a_n$ *(not all zero) though some may be zero such that*

$$a_1\alpha_1+a_2\alpha_2 \ldots +a_n\alpha_n=0 \qquad \textbf{Pb. 66} \quad \ldots(1)$$

Linearly independent. *If however the relation (1) implies that all the scalars* $a_1, a_2 \ldots a_n$ *are zero*

i.e. $\Sigma a_i\alpha_i=0 \Rightarrow a_i=0$ *for each i, then the set is said to be linearly independent (L. I.).*

From above definition of L. I. of a finite set, we conclude that an infinite set of vectors of V is L. I. if every finite sub set of this set is L. I. **(Pb. 69)**

Deductions.

(A) *Prove that a set of vectors which contains at least one zero vector is L. D.*

Let α_1 be a zero vector and $\alpha_2, \alpha_3 \ldots \alpha_n$ are all non zero vectors.

Consider the linear combination

$$1.\alpha_1+0\alpha_2+0\alpha_3 \ldots +0\alpha_n.$$

The above combination is zero because by definition $0.\alpha=0$ and $a.0=0$

$\therefore \quad 1.\alpha_1+0\alpha_2+0\alpha_3 \ldots +0\alpha_n=0 \quad \because \quad \alpha_1=0$

or $\quad \Sigma a_i\alpha_i=0$ where $a_1=1\neq 0$.

Hence by definition the given set which contains at least one zero vector is linearly dependent

B. *The singleton set* $\{\alpha_1\}$ *is L. I. iff* $\alpha_1\neq 0$

Let $\alpha_1\neq 0$ then $a.\alpha_1=0 \Rightarrow a=0 \quad \because \quad 0.\alpha_1=0$ by def.

Thus a linear combination of he vectors (here only one) is zero when all the scalars (here only one) are zero and as such it is linearly independent.

If $\alpha_1=0$ then it is linearly dependent by *A*

C. **Any sub set** *of a L. I. set is L. I.*

Let $\{\alpha_1, \alpha_2 \ldots \alpha_m\}$ be *a* L. I. set so that

$$a_1\,\alpha_1+a_2\,\alpha_2+\ldots+a_m\,\alpha_m=0$$
$$\Rightarrow a_1=0,\ a_2=0,\ldots\ldots,a_m=0$$

Consider the sub set $\{\alpha_1\ \alpha_2\ldots\alpha_k\}$ $1\leqslant k\leqslant m$.

If it is to be L. I. then there must exist scalars such that

$$a_1\,\alpha_1+a_2\,\alpha_2+\ldots+a_k\,\alpha_k=0 \qquad \ldots(1)$$

with $$a_1=a_2=\ldots=a_k=0$$

Now (1) can be expressed as

$$a_1\,\alpha_1+a_2\,\alpha_2+\ldots+a_k\,\alpha_k+0\,\alpha_{k+1}+\quad+0\,\alpha_m=0 \qquad \ldots(2)$$

But because $\{\alpha_1, \alpha_2\ldots\alpha_m\}$ is L.I. therefore each of the scalars in (2) should be zero.

$$\therefore\quad a_1=a_2=\ldots=a_k=0.$$ Hence Proved.

D. *Any super set of a. L.D. set is L.D.*

Let $\{u_1, u_2\ldots u_m\}$ be L.D. set so that

$$a_1\,u+a_2\,u_2+\ldots+a_m\,u_m=0$$

with at least one of the a^s not zero.

Suppose $a_i\neq 0$. Now consider the super set

$$\{u_1, u_2\ldots u_i\ldots u_m, u\}$$ then

$$a_1\,u_1+a_2\,u_2+\ldots+a_i\,u_i+\ldots+a_m\,u_m+au=0$$

and in the above combination there is at least one *i.e* a_i which is not zero and as such it cannot be L.I. but is L.D. by definition.

(c) *If the set* $\{u_1, u_2\ldots u_m\}$ *is L.I. set and if* $a_1, a_2, \ldots, a_m$ *and* $b_1, b_2, \ldots, b_m$ *be scalars* $\in F$ *such that*

$$a_1\,u_1+a_2\,u_2+\ldots+a_m\,u_m$$
$$=b_1\,u_1+b_2\,u_2+\ldots+b_m\,u_m$$

then $$a_1=b_1,\ a_2=b_2,\ a_3=b_3,\ \ldots,a_m=b_m.$$

From the given relation we conclude that

$$(a_1-b_1)\,u_1+(a_2-b_2)\,u_2+\ldots+(a_m-b_m)\,u_m=0$$

or $$A_1\,u_1+A_2\,u_2+\ldots+A_m\,u_m=0$$

Above is linear combination of the vectors of the given set which is L I, (given)

Hence $A_1=A_2=\ldots=A_m=0$

or $a_1-b_1=0,\ a_2-b_2=0,\ldots,a_m-b_m=0$

or $a_1=b_1,\ a_2=b_2,\ldots,a_m=b_m.$ **Proved**

(f) *If* $\alpha_1, \alpha_2,\ldots,\alpha_m \in V$ *and* $r_1, r_2,\ldots,r_m \in F$ *such that the set* $\{\alpha_2+r_2\,\alpha_1,\ \alpha_3+r_3\,\alpha_1,\ldots,\alpha_m+r_m\,\alpha_1\}$ *is* L.D. *then the set* $\{\alpha_1, \alpha_2\ldots\alpha_m\}$ *is also* L.D.

Since the given set is L.D., there exist scalars

$a_2, a_3,\ldots,a_m \in F$ such that

$a_2\,(\alpha_2+r_2\,\alpha_1)+a_3\,(\alpha_3+r_3\,\alpha_1)+\ldots+a_m\,(\alpha_m+r_m\,\alpha_1)=0$ ..(1)

with at least one of the a^s not equal to zero.

Rewriting (1) as below, we get

$(a_2\,r_2+a_3\,r_3+\ldots+a_m\,r_m)\,\alpha_1+a_2\,\alpha_2+\ldots+\alpha_m\,\alpha_m=0$

Above is a L.C. of the vectors of the set $\{\alpha_1, \alpha_2,\ldots,\alpha_m\}$ with at least one of the a^s not zero and hence it is L.D.

Exercise 4

Ex. 1. (a) *Prove that two vectors are linearly dependent if and only if one of them is a scalar multiple of the other*

α and β are L D. $\therefore$ $a\alpha+b\beta=0$

where both a and b are not zero.

Suppose $a\neq0$ then a^{-1} exists $\therefore$ $a^{-1}\,(a\alpha)+a^{-1}\,(b\beta)=0$

or $(a^{-1}\,a)\,\alpha=-(a^{-1}b)\,\beta$ or $\alpha=-\frac{b}{a}\beta$

Similarly if $b\neq0$ then $\beta=-\frac{a}{b}\alpha.$

i.e. one of them is a scalar multiple of the other.

If $\alpha=k\beta$ then $\alpha-k\beta=0$ where all the scalars are not zero and hence L.D.

(b) *Prove that the set of vectors* (*1, 3, 2*), (*1,−7,−8*), (*2, 1,−1*) *of* $V_3\,(R)$ *is linearly dependent.*

Let the given vectors be denoted by $\alpha_1, \alpha_2, \alpha_3$ respectively and let there be scalars a_1, a_2, a_3 belonging to R so that

$$\Sigma a_i \alpha_i = \mathbf{0} = (0, 0, 0)$$

$\therefore$ $a_1(1, 3, 2) + a_2(1, -7, -8) + a_3(2, 1, -1) = (0, 0, 0)$

$\therefore$ $(a_1, 3a_1, 2a_1) + (a_2, -7a_2, -8a_2) + (2a_3, a_3, -a_3)$
$= (0, 0, 0)$

$(a_1 + a_2 + 2a_3,\ 3a_1 - 7a_2 + a_3,\ 2a_1 - 8a_2 - a_3) = (0, 0, 0)$

$\therefore$ $\left.\begin{aligned} a_1 + a_2 + 2a_3 &= 0 \\ 3a_1 - 7a_2 + a_3 &= 0 \\ 2a_1 - 8a_2 - a_3 &= 0 \end{aligned}\right\}$ Eliminating a_3 we get $\left.\begin{aligned} 5a_1 - 15a_2 &= 0 \\ 5a_1 - 15a_2 &= 0 \end{aligned}\right\}$ or $a_1 = 3a_2$

i.e. if we choose $a_2 = 1$, then $a_1 = 3$ and putting in any we get $a_3 = -2$.

Hence the given system of vectors is linearly dependent.

(c) *Prove that the set of vectors*

$\alpha_1 = (0, 2, -4)$, $\alpha_2 = (1, -2, -1)$, $\alpha_3 = (1, -4, 3)$ *of* $V_3(R)$ *is linearly dependent.*

Proceeding as above we shall have

$\left.\begin{aligned} a_2 + a_3 &= 0 \\ 2a_1 - 2a_2 - 4a_3 &= 0 \\ -4a_1 - a_2 + 3a_3 &= 0 \end{aligned}\right\}$ Eliminating a_1 we get $a_2 + a_3 = 0$ and $-5a_2 - 5a_3 = 0$ *i.e.* $a_2 + a_3 = 0$

if we choose $a_2 = 1$, then $a_3 = -1$ and putting in any we get $a_1 = -1$.

Hence the given system of vectors is linearly dependent.

(d) *Prove that the system of four vectors*

$\alpha_1 = (1, 0, -1)$, $\alpha_2 = (2, 1, 3)$, $\alpha_3 = (-1, 0, 0)$, $\alpha_4 = (1, 0, 1)$ *of* $V_4(R)$ *are linearly dependent.*

Proceeding as above we shall have

$a_1 + 2a_2 - a_3 + a_4 = 0$
$a_2 = 0$
$-a_1 + 3a_2 + a_4 = 0$

Solving we get

$a_1 = a_1$, $a_2 = 0$, $a_3 = 2a_1$, $a_4 = a_1$

We can assign any value to a_1 and get the values of others.

Then all the a^s are not zero and hence the system is L.D.

(e) *Prove that the vectors* (a_1, a_2), (b_1, b_2) *of* $V_2(F)$ *are linearly dependent if* $a_1 b_2 - a_2 b_1 = 0$

Proceeding as above we get

$a a_1 + b b_1 = 0$ Eliminating a and b from these we get

$a a_2 + b b_2 = 0$ $\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = 0$ or $a_1 b_2 - a_2 b_1 = 0$

Above is the necessary and sufficient condition for the above equations to possess a non zero solution for a and b.

(f) *Prove that the four vectors*

$\alpha_1 = (1, 2, 3)$, $\alpha_2 = (1, 0, 0)$, $\alpha_3 = (0, 1, 0)$, $\alpha_4 = (0, 0, 1)$ *form a L.D. sub set of* $R^3(R)$.

Proceeding as above $a_1 = 1$, $a_2 = -1$, $a_3 = -2$, $a_4 = -3$.

Ex. 2. (a) *Show that the system of vectors*

$\alpha_1 = (1, 2, 0)$, $\alpha_2 = (0, 3, 1)$, $\alpha_3 = (-1, 0, 1)$ *of* $V_3(Q)$ *is L. I. when* Q *is the field of rational numbers,*

Choosing three scalars $a_1, a_2, a_3 \in Q$ we get

$$a_1 \alpha_1 + a_2 \alpha_2 + a_3 \alpha_3 = \mathbf{0} = (0, 0, 0)$$

$\therefore$ $(a_1 - a_3, 2a_1 + 3a_2, a_2 + a_3) = (0, 0, 0)$

or $a_1 - a_3 = 0$, $2a_1 + 3a_2 = 0$, $a_2 + a_3 = 0$

$\Rightarrow a_1 = 0$, $a_2 = 0$, $a_3 = 0$.

Hence linearly independent set.

(b) *Prove that the system of vectors*

$\alpha_1 = (0, 1, -2)$, $\alpha_2 = (1, -1, 1)$, *and* $\alpha_3 = (1, 2, 1)$ *are L. I.*

Proceeding as above we get

$$a_2 + a_3 = 0$$

$$a_1 - a_2 + 2a_2 = 0$$

$$-2a_1 + a_2 + a_3 = 0$$

From 1st and 3rd we get $a_1 = 0$

and from 1st and 2nd we get

$$a_2+a_3=0 \quad \therefore \quad 3a_3=0 \text{ or } a_3=0$$
$$-a_2+2a_3=0 \quad \text{and hence } a_2=0$$
$$\therefore \quad a_1=a_2=a_3=0 \text{ and hence L.I.}$$

(c) *Prove that the system of vectors belonging to vector space* F^n (F)

$$a_1=(1, 0, 0, \ldots,0),\ a_2=(0, 1, 0, 0, \ldots,0) \ldots \ldots a_n=(0, 0, 0,\ldots,1)$$

where I denotes the unity of field constitutes a L. I. set

$$a_1\,\alpha_1+a_2\,\alpha_2+\ldots+a_n\,\alpha_n=0=(0, 0, 0,\ldots,0)$$
$$\therefore \quad (a_1, a_2, \ldots, a_n)=(0, 0, 0,\ldots,0)$$

By definition of addition and scalar multiplication of n-tuples.

Above implies that each $a_i=0$ by definition of equality of n-tuples.

Hence L.I.

Ex. 3. *Show that in the vector space* $F(x)$ *of all polynomials in one indeterminate* x *over the field* F, *the infinite set* $1, x, x^2, x^3, \ldots$ *is a linearly independent set.*

We know from (c) P. 320 that

Any infinite set of vectors is said to be linearly independent if its every finite sub set is linearly independent.

Let $(1, x, x^2, \ldots, x^n)$ be a finite sub set of the given infinite set and $a_0, a_1, a_2, \ldots, a_n \in F$.

Then $a_0+a_1x+a_2x^2+\ldots+a_nx^n=0$ (zero polynomial).

Keeping in view the definition of zero polynomial and the equality of two polynomials, we get

$$a_0=0,\ a_1=0,\ a_2=0,\ \ldots,\ a_n=0.$$

Thus every finite sub set is L.I. and consequently the infinite set is also L. I.

Ex. 4. *Prove that the four vectors*

$\alpha_1=(1, 0, 0), \alpha_2=(0, 1, 0), \alpha_3=(0, 0, 1), \alpha_4=(1, 1, 1)$ *in* $V_3(C)$ *form a L.D. set but any three of them are L.I.* **(Meerut 69)**

Choosing $a_1, a_2, a_3, a_4 \in C$ we have

$$a_1\alpha_1+a_2\alpha_2+a_3\alpha_3+a_4\alpha_4=0$$

or $a_1(1, 0, 0)+a_2(0, 1, 0)+a_3(0, 0, 1)+a_4(1, 1, 1)=(0, 0, 0)$

$\therefore \quad (a_1+a_4, a_2+a_4, a_3+a_4)=(0, 0, 0)$

$\therefore \quad a_1+a_4=0, a_2+a_4=0, a_3+a_4=0.$

If $a_4=-k$ say then $a_1=a_2=a_3=k.$

$\therefore \quad k\alpha_1+k\alpha_2+k\alpha_3-k\alpha_4=0$ or $\alpha_1+\alpha_2+\alpha_3-\alpha_4=0$

showing that the given vectors are L.D.

2nd part. Let us show that $\alpha_1, \alpha_2, \alpha_4$ are L.I.

Let $a_1\alpha_1+a_2\alpha_2+a_4\alpha_4=0$

or $a_1(1, 0, 0)+a_2(0, 1, 0)+a_4(1, 1, ')=(0, 0, 0)$

$\therefore \quad a_1+a_4=0, a_2+a_4=0, a_4=0$

Since $a_4=0 \quad \therefore \quad a_2=a_1=0$

$\therefore \quad a_1\alpha_1+a_2\alpha_2+a_4\alpha_4=0 \Rightarrow a_1=a_2=a_4=0.$

Hence any three are linearly independent.

Ex. 5, *If* α, β, γ *are L. I. vectors in a vectar space* $V(F)$ *then prove that*

(a) $\alpha+\beta, \beta+\gamma, \gamma+\alpha.$

(b) $\alpha+\beta, \alpha-\beta, \alpha-2\beta+\gamma$ *are also L. I.*

Let $a(\alpha+\beta)+b(\beta+\gamma)+c(\gamma+\alpha)=0 \quad a, b, c \in F$

$a\alpha+a\beta+b\beta+b\gamma+c\gamma+c\alpha=0$

by laws of scalar multiplication in $V(F)$

or $\quad (a\alpha+c\alpha)+(a\beta+b\beta)+(b\gamma+c\gamma)=0$

or $\quad (a+c)\alpha+(a+b)\beta+(b+c)\gamma=0.$ As above

$\therefore \quad a+c=0, a+b=0, b+c=0$ as α, β, γ are L. I,

Solving $a=0$, $b=0$, $c=0$ and hence the given vectors constitute *a* L. I. set.

Similarly we can proceed for the second part.

Ex. 6. *Find the linearly independent sub set of the set* $S=\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ *in* $V_3(R)$ *where* $\alpha_1=(1, 2, -1)$, $\alpha_2=(-3, -6, 3)$, $\alpha_3=(2, 1, 3)$, $\alpha_4=(8, 7, 7)$ *which spans the same space as S.*

Let $\alpha \in L(S)$ $\therefore$ $\alpha=a_1\,\alpha_1+a_2\,\alpha_2+a_3\,\alpha_3+a_4\,\alpha_4$

Now $\alpha_2=-3\alpha_1$ and hence we can exclude α_2 so that

$$\alpha \in L(S)=b_1\,\alpha_1+b_3\,\alpha_3+b_4\,\alpha_4.$$

Again it can be easily verified that

$$\alpha_4=2\alpha_1+3\alpha_3$$

i.e. $(8, 7, 7)=2(1, 2, -1)+3(2, 1, 3)$

Hence we can exclude α_4 also so that

$$\alpha \in L(S)=c_1\,\alpha_1+c_3\,\alpha_3.$$

$\therefore$ $\{\alpha_1, \alpha_3\}$ spans the same space as S.

To prove. L. I. of $\{\alpha_1, \alpha_3\}$.

Let $c_1\,\alpha_1+c_3\,\alpha_3=\mathbf{0}$ $\quad c_1, c_3 \in R$.

$\therefore$ $c_1(1, 2, -1)+c_3(2, 1, 3)=(0, 0, 0)$

$\Rightarrow (c_1+2c_3, 2c_1+c_3, -c_1+3c_3)=(0, 0, 0)$

$\Rightarrow c_1+2c_3=0,\ 2c_1+c_3=0,\ -c_1+3c_3=0$

Solving we find that $c_1=0$, $c_3=0$ $\therefore$ $\{\alpha_1, \alpha_3\}$ is L. I.

Ex. 7. *If* $V(R)$ *be a vector space of* 2×3 *matrices over R then show that the matrices A, B, C given below are L. I.*

$$A=\begin{bmatrix} 2 & 1 & -1 \\ 3 & -2 & 4 \end{bmatrix},\quad B=\begin{bmatrix} 1 & 1 & -3 \\ -2 & 0 & 5 \end{bmatrix},$$

$$C=\begin{bmatrix} 4 & -1 & 2 \\ 1 & -2 & 3 \end{bmatrix}.$$

Choosing a, b, c as scalars $\in R$ we have

$a\,A+b\,B+c\,C=O_{2\times 3}$ *i.e.* null matrix of 2×3 type.

By rule of addition and scalar multiplication of matrices we have

$$\begin{bmatrix} 2a+b+4c & a+b-c & -a-3b+2c \\ 3a-2b+c & -2a-2c & 4a+5b+3c \end{bmatrix}$$
$$= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

By definition of equality of matrices we have

$2a+b+4c=0$ ...(1) $a+b-c=0$ ...(2)

$-a-3b+2c=0$ ...(2) $3a-2b+c=0$ .. (4)

$-2a-2c=0$ ...(5) $4a+5b+3c=0$ ...(6)

Eliminating c beween (2) and (5) we get $2a+b=0$ and hence from (1) we get $c=0$ and again from (5) we get $a=0$ and then from any other we get $b=0$,

Thus $a\ A+b\ B+c\ C=O_{3\times3}$ if $a=0$, $b=0$, $c=0$.

Hence the given matrices are linearly independent.

Theorem 9. Theorem on Linear Dependence.

The set of non zero vectors $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *of* $V(F)$ *is L.D. if and only if one of them say* α_k, $2 \leqslant k \leqslant n$ *can be expressed as a linear combination of the vectors which preceede it.*

(B. H. U. 70)

The condition is necessary.

Suppose that the set of n vectors $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is L. D., then by definition there exists scalars $a_1, a_2, \ldots, a_n$ (not all zero) such that

$$a_1\ \alpha_1+a_2\ \alpha_2+\ldots+a_k\ \alpha_k+\ldots+a_n\ \alpha_n=0$$

Again suppose that a_k is the last non zero coefficient,

If $k=1$ then $a_1\ \alpha_1=0$ but $a_1\neq0$, $\therefore\ \alpha_1=0$ which is a contradiction as the given set is of non zero vectors and hence

k will lie between 2 and n and at the most k could be equal to n, then

$$a_1\alpha_1+a_2\alpha_2+\ldots+a_k\alpha_k=0\ (a_k\neq0)$$

or $$a_k\alpha_k=-a_1\alpha_1-a_2\alpha_2-\ldots-a_{k-1}\alpha_{k-1}$$

or $$\alpha_k=-\frac{a_1}{a_k}\ \alpha_1-\frac{a_2}{a_k}\ \alpha_2\ldots-\frac{a_{k-1}}{a_k}\alpha_{k-1}.$$

Thus the vector a_k is a combination of the vectors which preceed it.

Conversely. Suppose any vector a_k can be expressed as a linear combination of the vectors preceeding it *i.e.*

$$a_k = -\frac{a_1}{a_k}a_1 - \frac{a_2}{a_k}a_2 - \ldots - \frac{a_{k-1}}{a_k}a_{k-1} \quad (a_k \neq 0)$$

or $$a_1a_1 + a_2a_2 + \ldots + a_ka_k = \mathbf{0} \quad \therefore \quad \{a_1, a_2, \ldots, a_n\} \text{ is L.D.}$$

Hence the set $\{a_1, a_2, \ldots, a_n\}$ which is a sub set of a *L*.D. set is also a L.D. set.

Cor. The set $S=\{a_1, a_2, \ldots, a_n\}$ of **non zero** vectors of $V(F)$ is L.D. iff one of these vectors can be expressed as a linear combination of the remaining $n-1$ vectors.

§ 11. Bases.

Definition. *If S is a sub set of a vector space $V(F)$, such that*

(a) S is linearly independent set of vectors in V.

(b) Every vector in V is a linear combination of elements of S or in other words $L(S)=V$, i.e. linear span of S is V, then S is called a basis (or a coordinate system) of $V(F)$. **(Aligarh 95; Pb. 69)**

Note We know that a set containing **zero** vector is L.D. set and hence by virtue of condition (a) above such a set cannot be basis set.

or **a zero vector cannot be an element of any basis set.**

Exercise No. 5

Ex. 1. *Show that the set of n vectors*

$e_1=(1, 0, 0, \ldots 0)$, $e_2=(0, 1, 0, 0, \ldots 0), \ldots, e_n=(0, 0, \ldots, 1)$

is a basis of $V_n(F)$.

Let $S=\{e_1, e_2, ..., e_n\}$, then S will be a basis set of $V_n(F)$ if S is linearly independent and $L(S)=V$, *i e.* each vector in V is a linear combination of elements of S.

For linear independence.

$$a_1e_1+a_2e_2+...+a_ne_n=0=\{0, 0, ...,0\}$$

or $a_1(1, 0, 0, ..., 0)+...--a_n(0, 0, ...1)=(0, 0, ...,0)$

or $(a, 0, 0, .., 0)+...+(0, 0, 0, ...a_n)=(0, 0, ..., 0)$

or $(a_1, a_2, ...,a_n)=(0, 0, 0, ...,0)$

$\Rightarrow a_1=0, a_2=0, ...,a_n=0.$

Hence the set S is *L. I.* set of vectors.

For L (S)=V.

Let $(a_1, a_2, ...,a_n)$ be any vector $\in V$, then as proved above $(a_1, a_2, ..., a_n)=a_1e_1+a_2e_2+...+a_ne_n$

or $\alpha \in V$ is expressible as a linear combination of elements of S, *i.e.* $V \subset L(S)$. Also we know that $L(S) \subset V$

$\therefore \quad L(S)=V$

Hence S is a basis set of $V_n(F)$.

$a_1, a_2, ...,a_n$ are called the **coordinates of vector** $(a_1, a_2, .. ,a_n) \in V_n(F)$ w. r. t. basis S.

Similarly we can prove that the set of unit vectors.

$\{(1, 0, 0), (0, 1, 0)$ and $(0, 0, 1)\}$ is a basis of $V_3(F)$.

and $\{(1, 0), (0, 1)\}$ is a basis for $V_2(F)$.

and the set $\{1\}$ is a basis for $F(F)$

where 1 is the unit element of F.

Ex. 2. *Prove that the set*

$$S=\{1, 2, 1), (2, 1, 0), (1, -1, 2)\}$$

forms a basis for $V_3(F)$.

For L.I.

$a_1\alpha_1+a_2\alpha_2+a_3\alpha_3=\mathbf{0}=(0, 0, 0)$

$\Rightarrow a_1(1, 2, 1)+a_2(2, 1, 0)+a_3(1, -1, 2)=(0, 0, 0)$

$$\Rightarrow (a_1+2a_2+a_3,\ 2a_1+a_2-a_3,\ a_1+2a_3)=(0,\ 0,\ 0)$$

$$\Rightarrow \left.\begin{aligned} a_1+2a_2+a_3&=\\ 2a_1+a_2-a_3&=0\\ a_1+2a_3&=0 \end{aligned}\right\} \Rightarrow a_1=0,\ a_2=0,\ a_3=0.$$

Hence S is L.I.

Now we have to establish that each vector in V can be expressed as a L C. of the elements of S.

Now any vector of

$$V_3(F)=(a_1, a_2, a_3)$$
$$=a_1(1, 0, 0)+a_2(0, 1, 0)+a_3(0, 0, 1), \quad \ldots(1)$$

where $(1, 0, 0)=x(1, 2, 1)+y(2, 1, 0)+z(1, -1, 2)$

$$=(x+2y+z,\ 2x+y-z,\ x+2z),$$

$\therefore \quad x+2y+z=1,\ 2x+y-z=0,\ x+2z=0.$

Solving we get

$$x=-\tfrac{2}{9},\ y=\tfrac{5}{9},\ z=\tfrac{1}{9}$$

$\therefore \quad (1, 0, 0)=-\tfrac{2}{9}(1, 2, 1)+\tfrac{5}{9}(2, 1, 0)+\tfrac{1}{9}(1, -1, 2).$

Similarly $(0, 1, 0)=\tfrac{4}{9}(1, 2, 1)-\tfrac{1}{9}(2, 1, 0)-\tfrac{2}{9}(1, -1, 2)$

$(0, 0, 1)=\tfrac{1}{3}(1, 2, 1)-\tfrac{1}{3}(2, 1, 0)+\tfrac{1}{3}(1, -1, 2)$

Hence from (1) on putting for unit vectors, we get that (a_1, a_2, a_3) can be expressed as a linear combination of the elements of S.

Therefore S is a basis set of $V_3(F)$.

Ex. 3. *Show that the set* $S=\{1, x, x^2, \ldots, x^n\}$ *of n polynomials is a basis set for the vector space* $P_n(R)$ *of all polynomials (of degree at most n) over the field of real numbers.*

For linear independence of S.

For $a_0, a_1, a_2, \ldots, a_n \in F$ *i.e.* R, we have

$$a_0\,1+a_1x+a_2x^2+a_3x^3+\ldots+a_nx^n=0,$$

i.e. zero polynomial

$$\Rightarrow a_0=0,\ a_1=0,\ a_2=0,\ \ldots, a_n=0.$$

Hence S is L.I. set of vectors.

Again any polynomial $\in P_n(R)$ say,

$$a_0+a_1x+a_2x^2+...+a_nx^n$$

is a linear combination of the elements $1, x, x^2,..., x^n$ of S.

$\therefore$ S is a basis set of $P_n(R)$.

Ex. 4. *Prove that the set*

$$S\{(1, 0, 0), (1, 1, 0), (1, 1, 1), (0, 1, 0)\},$$

spans the vector space $R^3(R)$ *but is not a basis set.*

Here we shall show that $L(S)=R^3(R)$, *i.e.* S is a spanning set but S is not L.I., so that S will not be a basis set of $R^3(R)$.

In order to prove that $L(S)=R^3(R)$, we know that

$L(S)$ is a sub set of $R^3(R)$ **(Theorem 9·1 P. 237)** ...(1)

and we shall now show that $R^3(R)$ is a sub set of $L(S)$, *i.e.* any element $(a_1, a_2, a_3) \in R^3(R)$ can be expressed as L.C. of vectors in S.

Let $(a_1, a_2, a_3)=x(1, 0, 0)+y(1, 1, 0)+z(1, 1, 1)$
$+\omega(0, 1. 0)$

$$=(x+y+z, y+z+\omega, z)$$

$\Rightarrow x+y+z=a_1, y+z+\omega=a_2, z=a_3.$

$\therefore$ $z=a_3, y=a_2-z-\omega=a_2-a_3-\omega, x=a_1-a_2+\omega.$

Choose $\omega=0$, we get

$$z=a_3, y=a_2-a_3, x=a_1-a_2.$$

$\therefore$ $(a_1, a_2, a_3)=(a_1-a_2)(1, 0, 0)+(a_2-a_3)(1, 1, 0)$
$+a_3(1, 1, 1)+0(0, 1, 0).$

$$\therefore \quad R^3(R) \subseteq L(S). \qquad ...(2)$$

Hence from (1) and (2) we prove that $L(S)=R^3(R)$.

Again in order to prove that S is not L.I., let us suppose that

$x(1, 0, 0)+y(1, 1, 0)+z(1, 1, 1)+\omega(0, 1, 0)=0$
$=(0, 0, 0).$

$$\therefore \quad (x+y+z,\ y+z+\omega,\ z)=(0,\ 0,\ 0).$$
$$\therefore \quad x+y+z=0,\ y+z+\omega=0,\ z=0.$$
$$\therefore \quad z=0,\ y=-\omega,\ x=\omega.$$

In particular choosing $\omega=1$, we get

$$x=1,\ y=-1,\ z=0,\ \omega=1.$$
$$\therefore \quad 1\ (1,\ 0,\ 0)+(-1)\ (1,\ 1,\ 0)+(1,\ 1,\ 1)+1\ (0,\ 1,\ 0) = (0,\ 0,\ 0).$$

i.e. $$\Sigma\ a_i\alpha_i=0,$$

where all a_is are not zero.

Hence S is not L.I. but is L.D. set.

Ex. 5. *If V be the vector space of ordered pairs of complex numbers over the real field R, then show that the set.*

$S=\{(1,\ 0),\ (i\ ,\ 0),\ (0,\ 1),\ (0,\ i)\}$ is a basis of V.

S is a L.I. set.

$$a\ (1,\ 0)+b\ (i,\ 0)+c\ (0,\ 1)+d\ (0,\ i)=(0,\ 0)$$
$$\Rightarrow\ (a+ib,\ c+id)=(0,\ 0)$$
$$\Rightarrow\ a+ib=0,\ c+id=0$$
$$\Rightarrow\ a=0,\ b=0,\ c=0,\ d=0.$$ Hence L. I.

L (S)=V.

Let any ordered pair $(a+ib,\ c+id) \in V$

Then as shown above $(a+ib,\ c+id)$

$$=a\ (1,\ 0)+b\ (i,\ 0)+c\ (0,\ 1)+d\ (0,\ i)$$

i.e. any vector in V is expressible as a L.C. of elements of S.

$\therefore \quad V \subset L\ (S)$. Also $L\ (S) \subset V \quad \therefore \quad L(S)=V$

Hence S is a basis set.

Note. a, b, c, d are **the coordinates of the vector** $(a+ib,\ c+id)$ w. r. t. basis S.

Ex. 6. *Prove that the set $S=\{(1,\ 0,\ 0),\ (1,\ 1,\ 0),\ (1,\ 1,\ 1)\}$ is a basis set for vector space $V_3\ (C)$ and hence find the coordi-*

nates of the vector $(3+4i,6i,3+7i)$ *in* $V_3(C)$ *w.r.t. above basis.*

Considering the relation

$a(1, 0, 0)+b(1, 1, 0)+c(1, 1, 1)=(0, 0, 0)$ we get

$a+b+c=0,\ b+c=0,\ c=0 \Rightarrow a=b=c=0 \therefore$ L.I.

Again let $(a, b, c) \in V_3(C)=p(1, 0, 0)+q(1, 1, 0)+r(1, 1, 1)$

$\therefore\ p+q+r=a,\ q+r=b,\ r=c$

$\therefore\ q=b-c$ and $p=a-b$

$\therefore\ (a, b, c)=(a-b)(1, 0, 0)+(b-c)(1, 1, 0)+c(1, 1, 1)$

Thus the given set is a spanning set and it being L.I. also therefore constitutes a basis.

Now putting $a=3+4i,\ b=6i,\ c=3+7$

we get $p=a-b=3-2i,\ q=b-c=-3-i,\ r=c=3+i$

$\therefore\ (3+4i, 6i, 3+7i)=(3-2i)(1, 0, 0)+(-3-i)(1, 1, 0)+(3+7i)(1, 1, 1)$

Hence the coordinates of the given vector are

$3-2i,\ -3-i,\ 3+7i$ w.r.t. basis S

Ex. 7. *Prove that the set* $S=\{\alpha+i\beta,\ \gamma+i\delta\}$ *is a basis set of* $C(R)$ *iff* $\alpha\delta-\beta\gamma\neq 0$.

For L.I. of S $a(\alpha+i\beta)+b(\gamma+i\delta)=0$

$\Rightarrow a\alpha+b\gamma=0,\ a\beta+b\delta=0$ ...(1)

$\Rightarrow a\alpha\beta+b\gamma\beta=0$ and $a\beta\alpha+b\delta\alpha=0$

$\Rightarrow a\alpha\beta+b\gamma\beta=a\beta\alpha+b\delta\alpha \Rightarrow b(\gamma\beta-\delta\alpha)=0$

$\Rightarrow b=0$ provided $\gamma\beta-\delta\alpha\neq 0$ or $\alpha\delta-\beta\gamma\neq 0$

Also when $b=0$ then from (1) $a=0$ and hence S is L.I. set if $\alpha\delta-\beta\gamma\neq 0$.

Again let $\theta+i\phi \in c(R)=a(\alpha+i\beta)+b(\gamma+i\delta)$

$\Rightarrow \theta=a\alpha+b\gamma,\ \phi=a\beta+b\delta$

Solving these we get

$$a=\frac{\theta\delta-\phi\gamma}{\alpha\delta-\beta\gamma},\quad b=\frac{\theta\beta-\alpha\phi}{\gamma\beta-\delta\alpha}$$

provided $\alpha\delta-\beta\gamma\neq 0$.

Hence any element $\in C(R)$ is expressible as $a\ l.c.$ of elements of S *i e.* $C(R)=L(S)$ if $\alpha\delta-\beta\gamma=0$.

Hence S is a basis set if the above condition is satisfied.

Ex. 8. *T_1, T_2, T_3 are linear transformations belonging to the vector space $L(R^3, R^2)$ defined as*

$T_1(x, y, z)=(x+y+z, x+y)$, $T_2(x, y. z)=(2x+z, x+y)$

$T_3(x, y, z)=(2y, x)$. *Prove that T_1, T_2, T_3 are linearly independent.*

Consider $a\,T_1+b\,T_2+c\,T_3=O$ *i.e.* zero transformation.

$\therefore\quad (a\,T_1+b\,T_2+c\,T_3)\,\alpha=O\ (\alpha)=(0, 0)\qquad \forall\ \alpha\in R^3$

Choosing $\alpha=e_1=(1, 0, 0)$ and $e_2=(0, 1, 0)$ we get

$$a\,T_1(e_1)+b\,T_2(e_1)+c\,T_3(e_1)=(0, 0)$$

$$a\,T_1(e_2)+b\,T_2(e_2)+c\,T_3(e_2)=(0, 0)$$

$\therefore\quad a(1, 1)+b(2, 1)+c(0, 1)=(0, 0)$

putting $x=1, y=0, z=0$

$$a(1, 1)+b(0, 1)+c(2, 0)=(0, 0)$$

or $(a+2b, a+b+c)=(0, 0)$ putting $x=0, y=1, z=0$

and $(a+2c, a+b)=(0, 0)$

$\therefore\quad a+2b=0,\ a+b+c=0,\ a+2c=0,\ a+b=0$

Above relation when solved give $a=b=c=0$

and hence $a\,T_1+b\,T_2+c\,T_3=O \Rightarrow a=0, b=0, c=0$

and hence T_1, T_2, T_3 are linearly independent.

§ 12·1. Finite dimensional vector space or finitely generated.

Definition. *A vector space $V(F)$ is said to be finitely generated if there exists a finite sub set S of V such that*

$$V=L(S)$$

or in other words if $V(F)$ has a finite spanning set.

Theorem 10. *In a finite dimensional vector space $V(F)$ whose basis set $B=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ every vector $\alpha \in V$ is uniquely expressible as a linear combination of the vectors in B.*

In other words we have to show that corresponding to a given vector $\alpha \in V$ and a given basis B there exists a unique set of scalars a_i s.t. $\alpha=\sum_{i=1}^{n} a_i \alpha_i$.

Proof. Since B is a basis set of $V(F)$.

$\therefore \quad \alpha \in V=\Sigma \alpha_i a_i,\ a_i \in F.$ ...(1)

We have to show that the scalars a_i are unique and if not let there be any other set b_i of scalars such that

$$\alpha \in V=\Sigma b_i a_i. \qquad \ldots(2)$$

from (1) and (2) we get

$$\Sigma a_i \alpha_i=\Sigma b_i \alpha_i \text{ or } \Sigma (a_i-b_i)\alpha_i=\mathbf{0} \qquad \ldots(3)$$

Since B being a basis set is linearly independent and hence we have from (3)

$a_i-b_i=0 \ \forall \ i$ *i.e.* $a_1=b_1,\ a_2=b_2, \ldots, a_n=b_n$.

Hence the set of scalars is unique and the unique set of scalars are called the **coordinates** of vector α w. r. t. **given basis B.**

It should be clearly understood here that these coordinates of a vector α are unique only w. r. t. the basis B and in case we have another basis B' then the coordinates of the vector α would be different.

Illustration.

Consider the vector space $V_3(R)$ and we have proved earlier that the two L. I. sets.

$B=\{(1, 0, 0), (0, 1, 0), (0, 0, 1)\}$

$B'=\{(1, 0, 0), (1, 1, 0), (1, 1, 1)\}$ are basis sets

(see Ex. 6 P. 333)

$(a, b, c) \in V_3(R)=a(1, 0, 0)+b(0, 1, 0)+c(0, 0, 1)$

So the coordinates of (a, b, c) w.r.t. basis B are a, b, c.

Also $(a, b, c) \in V_3(R)$

$=(a-b)(1, 0, 0)+(b-c)(1, 1, 0)+c(1, 1, 1)$

as can be verified.

So the coordinates of (a, b, c) w.r.t. basis B' are

$$a-b, b-c, c.$$

Theorem 10. Existence Theorem.

There exists a basis for each finite dimensional vector space. **(Meerut M. Sc. 67, 69, 71)**

As $V(F)$ is finite dimensional vector space therefore by definition there exists a finite sub set $S=\{\alpha_1, \alpha_2, ..., \alpha_n\}$ such that $L(S)=V$ *i.e.* each vector in V is expressible as a l. c. of vectors in S.

We may suppose here without any loss of generality that none of the vectors in S is a zero vector because in any linear combination of vectors of S the contribution of zero vector would be zero as $a.0=0$

In case S is a linearly independent set then this fact combined with the fact that $L(S)=V$ makes the set S a basis set. In case S is not L. I. set then it is linearly dependent set. Since S is L. D. we have by Th. 9 P. 327 any vector α_k is expressible as a l.c. of the vectors which preceede it.

.. (1)

i.e. $\alpha_k=$ l. c. of $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$

Consider the set $S_1=\{\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_n\}$.

Clearly $S_1 \subset S \quad \therefore \quad L(S_1) \subset L(S) \subset V \quad \because \quad V=L(S)$

.. (2)

$\therefore \quad L(S_1) \subset V$

Now we shall show that $V \subset L(S_1)$

Let $\alpha \in V$=l.c. of $\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots, \alpha_n$ $\because L(S)=V$

=l.c. of $\{\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_n\}+a_k\ \alpha_k$

=l.c. of elements of S_1+a_k (l.c. of $\alpha_1, \alpha_2, \ldots, \alpha_{k-1}$), by I

=l.c. of elements of S_1 and hence $\alpha \in L(S_1)$

$\therefore \quad \alpha \in V \Rightarrow \alpha \in L(S_1) \qquad \therefore \quad V \subset L(S_1) \qquad \ldots (3)$

Hence from (2) and (3) we conclude that $V=L(S_1)$

Now if S_1 is L. I. and also $V=L(S_1)$ then S_1 is a basis set of V.

But if S_1 is also L. D. then proceeding as above we can have a set S_2 of $n-2$ vectors such that $L(S_2)=V$ and in case S_2 is L. I. then S_2 is a basis set. If not then continuing as above for a finite steps we shall obtain a set T such that $L(T)=V$ and T is also L. I. and this set T will constitute a basis for V.

It may happen that in the above process we may be left with a sub set which contains a single non zero vector and which spans V. From (B) P. 320 we know that a singleton $\{\alpha\}$ is L.I. iff $\alpha \neq 0$. Hence this will form a basis.

Another form of the above Theorem. *If a finite set S of vectors spans a finite dimensional vector space $V(F)$ then there exists a sub set T of S which forms a basis of V.*

Theorem 11. Invariance of the number of element of a basis set.

If $V(F)$ be a finite dimensional vector space then any two basis of V have the same number of elements.

(Punjab 67, 69; Kanpur 69; Meerut B. Sc. 70, M. Sc. 69)

Let $B_1=\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$.

$B_2=\{\beta_1, \beta_2, \ldots, \beta_n\}$.

be two basis of $V(F)$ consisting of m and n elements respectively and we shall prove that $m=n$.

Since B_1 is a basis set $\therefore \quad V=L(B_1)$. *i.e.* any vector in V

can be expressed as a l. c. of the vectors in B_1. Now $\beta_1 \in V$ and hence β_1 = l.c. of $(\alpha_1, \alpha_2, \ldots\ldots, \alpha_m)$.

or $S = \{\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a linearly dependent set. Therefore there exists a vector α_k such that

α_k = l. c. of preceeding vectors $\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}$ ...(1)

Now $V = L(B_1)$ $\therefore$ $\alpha \in V$ = l.c. of $\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots, \alpha_m$.

or $\alpha \in V$ = l.c. of $(\alpha_1\ \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ \ , \alpha_m) + a_k \alpha_k$.

= l.c. of $(\alpha_1, \alpha_2 \cdot \alpha_{k-1}, \alpha_{k+1} \ldots \alpha_m)$
$+ a_k$ (l.c. of $\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}$) by I

= l.c. of $\{\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1} \alpha_{k+1}, \ldots, \alpha_m\}$

= l.c. of elements of S_1

where $S_1 = \{\beta_1, \alpha_1, \alpha_2\ \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_m\}$ ...(2)

Hence $V(F)$ is also spanned by the above set S_1 wnich is obtaind by omitting one α and adding one β to the vectors in B_1. *i e.* $V = L(S_1)$

Again $\beta_2 \in V$ and S_1 is a spanning set for $V(F)$ and as such

β_2 = l.c. of elements of S_1, *i.e.* $\{\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_m\}$

$\therefore$ $\{\beta_2, \beta_1, \alpha_1, \alpha_2 \cdot \alpha_{k-1}, \alpha_{k+1} \ldots \alpha_m\}$ is a linearly dependent set.

Hence there exists a vector α_j (different from β_2 and β_1) such that

α_j = l.c of preceeding vectors $\{\beta_2, \beta_1, \alpha_1, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots \alpha_{j-1}\}$ ...(3)

Now $V = L(S_1)$ $\therefore$ $\alpha \in$

V = l.c. of $\{\beta_1, \alpha_1, \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_m\}$

= l.c of $(\beta_1, \alpha_1, \alpha_3, \alpha_2, \ldots, \alpha_{k-1}, \alpha_{k+1}, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_m\}$
$+ a_j\ \alpha_j$

= l.c of (,..., ...) $+ a_j$ (l.c of $\beta_2, \beta_1, \alpha_1$
..., $\alpha_{k-1}, \alpha_{k+1}, \alpha_{j-1}$) by (3)

= l.c of elements of S_2

where $S_2 = \{\beta_2, \beta_1, \alpha_1, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_{j-1}, \alpha_{j+1}, \ldots, \alpha_m\}$ .. (4)

Hence $V(F)$ is also spanned by set S_2 which is obtained by omitting one α and adding one β to the set S_1.

Continuing the process we shall at each stage exclude one α and include one β so that the resulting set is a spanning set.

No we argue that the set B_1 of α^s consisting of m vectors can not be exhausted before the set B_2 of β^s consisting of n vectors is exhausted because in that case we shall obtain a spanning set S_m which will consist only of β^s and none of the α^s. This would mean that S_m which is a proper sub set of the basis set B_2 of β^s generates $V(F)$ which is not possible,

Hence the number of vectors α^s in B_1 can not be less than the number of vectors β^s in B_2 *i.e.* $m \not< n$. ...(5)

Now if we interchange the role of basis B_1 and B_2 and argue as above *i.e.* we start excluding one of the β^s and go on adding one of the α^s we shall get that $n \not< m$. ...(6)

Hence from (5) and (6) we obtain that $m=n$.

Hence Proved.

The above theorem is also known as replacement theorem.

§ 13. Dimensions of a vector space

Deffnition. *The dimensions of a finite dimensional vector space $V(F)$ is the number of elements in a basis of $V(F)$ and is denoted as dim V.*

For example dim $R^n(R)=n$, as $(e_1, e_2, \ldots, e_n)$ is a basis set of above consisting of n elements.

Theorem 12. Extension Theorem.

If $V(F)$ is a finite dimensional vector space and $A=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is any set of L. I. vectors of V, then unless the α^s already form a basis we can find the vectors $\{\beta_1, \beta_2, \ldots\ldots, \beta_{n-m}\}$, so that the extended set of n vectors $\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_{n-m}\}$ is a basis

Thus every L. I. set can be extended to from a basis.

(Delhi Hon's 69; Aligarh 65; Kanpur 69; Meerut 68)

Proof Since $V(F)$ is finite dimensional, there exists a basis of V (Th. 10· P. 337) which will consist of say n elements and let

$B=\{\beta_1, \beta_2, \ldots, \beta_i, \ldots, \beta_n\}$ be a basis set

so that $V=L(B)$ and B is a L. I. set.

Also it is given that the set $A=\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a L. I. set nd as such none of the α^s can be expressed as a l.c. of the preceeding α^s in A.

Also each of the α^s is a member of V and as such it can be expressed as a l.c. of elements of basis set B.

$$i.e. \qquad \alpha_j = \text{l.c. of } \beta^s \text{ in } B \qquad \ldots(1)$$

Now consider the set

$S=\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_n\}$ of $m+n$ vectors.

which is obtained by extension of the given L.I. set A.

We shall show that $L(S)=V$ and if S is also L.I. then the extended set will be a basis otherwise not.

Let $\alpha \in V \Rightarrow \alpha = \text{l.c. of } \beta^s = \sum_{i=1}^{n} b_i \beta_i$

$$= \sum_{i=1}^{m} 0_i \alpha_j + \sum_{i=1}^{n} b_i \beta_i$$

$$= \text{l.c. of elements of } S \Rightarrow \alpha \in L(S)$$

$\therefore \quad V \subset L(S)$.

Now let $\alpha \in L(S)$ $\quad \therefore \ \alpha = \text{l.c. of elements of } S$

$\Rightarrow \alpha = \text{l.c. of } \alpha_j^s + \text{l.c. of } \beta_i^s$

But by (1) each α_j^s is expressible as a l.c. of β_i^s

Hence $\alpha \in L(S) \Rightarrow \alpha = \text{l.c. of } \beta_i^s \Rightarrow \alpha \in V$.

$\therefore \quad L(S) \subset V$.

Hence $V=L(S)$.

But S is a L. D. set, because by (1)

$\alpha_j = \text{l.c. of } \beta^s = \Sigma\, b_i \beta_i$ and it can be expressed as

$$\alpha_j=\sum_{p=1}^{m} 0\ \alpha_p+\sum_{i=1}^{n} b_i\ \beta_i$$

$p\neq j$

i.e. l.c. of remaining $m+n-1$ vectors of S, and hence by Cor. to Th. 9. P. 329 S is a L. D. set

Now since S is L. D. therefore any vector of S can be expressed as a l.c. of the preceeding vectors. But none of the α^s in S can be so expressed as the set A is L. I. as shown above. Hence such a vector must be some one of the β^s in S and let it be β_t.

$\therefore\ \beta_t \in S$ which is L.D.=l.c. of $\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_{t-1}\}$ ...(2)

Now consider the set S_1 which consists of all the vectors of S except β_t.

$\therefore\quad S_1=\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_{t-1}, \beta_{t+1}, \ldots, \beta_n\}$

Now we shall show that $L(S_1)=V$ and if S_1 is L. I. also S_1 is a basis set which is obtained by extending the set A

Since $S_1 \subset S \therefore L(S_1) \subset L(S)$ and because $L(S) \subset V$

$\therefore\quad L(S_1) \subset V.$

For $V \subset L(S_1)$ let us choose

$$\alpha \in V \quad \therefore\ \alpha=\sum_{j=1}^{n} b_j\ \beta_j=\sum_{\substack{j=1\\ j\neq t}}^{n} b_j\ \beta_j+b_t\ \beta_t$$

$\Rightarrow$ α=l.c. of $(\beta_1, \beta_2, \ldots, \beta_{t-1}, \beta_{t+1}, \ldots, \beta_n)$
$+b_t$ [l.c. of $\{\alpha_1, \alpha_2 \ldots \alpha_m, \beta_1, \beta_2 \ldots \beta_{t-1}, \beta_{t+1} \ldots \beta_n\}$] by (2)
$\Rightarrow$ α=l.c. of elements of $S_1 \Rightarrow \alpha \in L(S_1)$
$\therefore\quad V \subset L(S_1).$ ...(4)

Hence from (3) and (4) we get $V=L(S_1)$

Now if S_1 is a L. I. set and since $V=L(S_1)$ therefore S_1 is a basis set which is an extension of given L. I. set A.

In case S_1 is L.D. then we can continue the process as ove and obtain another set S_2 in which one more β^s is eliminated whereas all the α^s remain which again is an extension of L.I. set A and we can show that $L(S_2)=V$ and if S_2 is L.I. then it will be basis and if not then continuing the process for a finite number of times we shall obtain a set S_m by eliminating m β^s so that the set

$S_m=\{\alpha_1, \alpha_2,\ldots,\alpha_m, \beta_1, \beta_2,\ldots,\beta_{n-m}\}$ consisting of $m+n-m=n$ vectors is such that

$$V=\mathrm{L}(S_m) \text{ and also } S_m=\text{L.I. set.}$$

This set S_m which is an extension of L.I. set A is a basis set for V consisting of n elements equal to the dimension of the given finite dimensional vector space.

Cor. 1. *Each sub set of $(n+1)$ or more vectors of an n-dimensional vector space $V(F)$ is linearly dependent.*

(Meerut M.Sc. 70, B.Sc. 69)

If the set consisting of $(n+1)$ or more vectors were L.I, then either it is itself a basis or it could be extended to form a basis of $V(F)$. It would mean in either case that the basis set of $V(F)$ will consist of $(n+1)$ or more vectors which contradicts the definition that $V(F)$ is n dimensional. Hence the sub set containing $n+1$ vectors is L.D.

Cor 2. *Every sub set consisting of n linearly independent vectors of an n dimensional vector space is a basis set.*

We have proved that every L.I set can be extended to form a basis. Since the vector space is n dimensional, its basis shall not consist of more than n elements. As such the given set consisting of n elements and which is L.I. cannot be further extended but it will itself form a basis.

Theorem 13. Dimension of a sub space of V (F).

Each sub space W of a finite dimensional vector space V (F) of dimension n is a finite dimensional vector space with dimension less than or equal to n. i.e. dim W ⩽ dim V.

(Marthwada 70, Delhi Hon's. 70, Meerut M.Sc. 69, B.Sc. 71)

Since dim $V(F)=n$, therefore any $n+1$ or more vectors in V will constitute a. L.D. set by Cor. 1. and as such any $(n+1)$ or more vectors in W are also L.D. Therefore a L.I. set of vectors in W will at the most contain n vectors.

Let the largest set of L.I. vectors in W be

$S=\{\alpha_1, \alpha_2,\ldots,\alpha_m\}$ where $m \leqslant n$.

Now we shall establish that this set S is a spanning set for W *i e.* $L(S)=W$ and it being L.I. will be a basis consisting of finite number of elements and hence W will be a finite dimensional vector space whose dimension is equal to $m \leqslant n$ where m is the number of elements in the basis set S.

Let $\alpha \in W$ then the set $S_1=\{\alpha, \alpha_1, \alpha_2,\ldots\ldots,\alpha_m\}$ is linearly dependent because the largest L.I. set in W contains only m elements.

Hence $a\alpha+a_1\alpha_1+a_2\alpha_2+\ldots+a_m\ \alpha_m=0$

$$a, a_i \in F \qquad \ldots(1)$$

$\Rightarrow$ that all a_i and a are not zero because otherwise the set S_1 would be L.I.

Our contention is that $a \neq 0$ because if

$a=0$ then from I

$\Sigma\, a_i\alpha_i=0 \Rightarrow$ all a_i's are zero because S is a L.I. set

Hence all a_i and a would be zero which is a contradiction. Hence our contention that $a \neq 0$ is true. Since $a \neq 0$ we can write (1) as

$$\alpha=-\left(\frac{a_1}{a}\alpha_1+\frac{a_2}{a}\alpha_2+\ldots+\frac{a_m}{a}\alpha_m\right)$$

or $\alpha \in W$=L.C. of elements of S *i.e.* $W=L(S)$.

Hence S is a basis set $\therefore$ W is finite dimensional

and $\dim W=m$

where $m\leqslant n$ $\therefore$ $\dim W\leqslant \dim V$

Deduction. Dim. $V=$Dim $W\Leftrightarrow V=W$.

In case $V=W$ then every basis of V is al o a basis of W $\therefore$ $\dim V=\dim W$.

Now let $\dim V=\dim W=n$ (say)

Let S be a basis for W consisting of n elements so that $L(S)=W$

Now S being basis for W is a sub-base of W' and W' is a sub group of V. Therefore S is subset of V and it contains n linearly independent vectors.

But $\dim V=n$ given so that this S must also be a basis for V and hence $L(S)=V$

Since $L(S)=W$, $L(S)=V$ $\therefore$ $V=W$.

Theorem 14. Dimension of direct sum.

If a finite dimensional (f.d.) vector space $V(F)$ be the direct sum of two sub spaces W_1 and W_2 then

$$\dim V=\dim W_1+\dim W_2.$$

Since V is $f.d$ therefore its sub spaces are also $f.d.$ and let $\dim W_1=l$ and $\dim W_2=m$ so that

$S_1=\{\alpha_1, \alpha_2, ..,\alpha_l\}$ is a basis for W_1 and

$S_2=\{\beta_1, \beta_2,...,\beta_m\}$ is a basis for W_2

where both S_1 and S_2 are linearly independent sets.

In order to prove that $\dim V=\dim W_1+\dim W_2=l+m$, we should show that the set $S_3=\{\alpha_1, ..,\alpha_l, \beta_1,...,\beta_m\}$ is a basis set for V and hence we will have to establish that

(*a*) S_3 is L I. (*b*) $V=L(S_3)$.

(*a*) Consider $\sum_{i=1}^{l} a_i \alpha_i+\sum_{j=1}^{m} b_j \beta_j=0$. (1)

$\Rightarrow \Sigma a_i \alpha_i=-\Sigma b_j \beta_j$.

L.H.S. is a vector in W_1 as S_1 is a basis for W_1 and R.H.S. is a vector in W_2 as S_2 is a basis for W_2 and both being equal we conclude that each of them belongs to both W_1 and W_2 and hence belongs to $W_1 \cap W_2$

$\therefore \quad \Sigma a_i \alpha_i \in W_1 \cap W_2$ and $-\Sigma b_g \beta_g \in W_1 \cap W_2$

or $\quad \Sigma b_g \beta_g \in W_1 \cap W_2$

Now $\quad V = W_1 \oplus W_2$ given $\Rightarrow W_1 \cap W_2 = \{0\}$

$\therefore \quad \Sigma a_i \alpha_i = 0, \quad \Sigma b_g \beta_g = 0$

$\Rightarrow a_i = 0 \ \forall \ i = 1,\ldots,l, \quad b_g = 0 \ \forall \ g = 1,\ldots,m.$ as both S_1, S_2 are L.I Sets being basis sets.

Hence from (1) we conclude that S_3 is a L.I. set

(*b*) $\quad V = L(S_3)$.

Since $V = W_1 \oplus W_2$. $\Rightarrow Z \in V = \alpha + \beta, \ \alpha \in W_1, \beta \in W_2$

$\Rightarrow Z = \Sigma a_i \alpha_i + \Sigma b_g \beta_g =$ L.C. of elements of S_3

$\Rightarrow Z \in L(S_3) \quad \therefore \quad V \subseteq L(S_3)$ ...(2)

Also $Z \in L(S_3) \Rightarrow Z = \Sigma a_i \alpha_i + \Sigma b_g \beta_g \Rightarrow Z = \alpha + \beta$

where $\alpha \in W_1, \quad \beta \in W_2 \Rightarrow Z \in V$

$\therefore \quad L(S_3) \subset V.$ ...(3)

Hence from (2) and (3) we get $L(S_3) = V$

$\therefore$ S_3 is a basis set for V containing $l+m$ vectors so that dim $V = l+m =$ dim $W_1 +$ dim W_2 **Proved**

Theorem 15. *Let V be a finite dimensional vector space and W_1, W_2 be sub-spaces of V such that $V = W_1 + W_2$ and dim V = dim W_1 + dim W_2 then $V = W \oplus W_2$*

V is finite dimensional $\Rightarrow$ its sub space W_1, W_2 are also finite dememional.

$\therefore \quad S_1^* = \{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ be a basis of W_1

$S_2 = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a basis of W_2

Consider the set $S_3 = \{\alpha_1, \alpha_2, \ldots, \alpha_l, \beta_1, \beta_2, \ldots, \beta_m\}$ of $l+m$ elements.

Since $\quad V = W_1 + W_2 \quad \therefore \quad Z = \alpha + \beta$

$\in V \quad \in W_1 \in W_2$

or $Z=\Sigma\, a_i\, \alpha_i+\Sigma\, b_i\, \beta_i$ as S_1 and S_2 are basis for W_1 and W_2 respectively.

or $Z=l.c.$ of S_3 and hence $L(S_3)=V$

Now dim $V=$dim W_1+dim $W_2=l+m$ and the set S_3 of $l+m$ elements which spans V must be a basis set for V. Therefore S_3 is linearly independent.

Now we have to show that $V=W_1 \oplus W_2$

Since $V=W_1+W_2$ given we have only to show $W_1 \cap W_2=\{0\}$

Let $\alpha \in W_1 \cap W_2 \Rightarrow \alpha \in W_1$ and $\alpha \in W_2$

$\therefore \quad \alpha=\Sigma\, a_i\, \alpha_i \qquad \alpha=\Sigma\, b_j\, \beta_i$

$\therefore \quad \Sigma\, a_i\, \alpha_i=\Sigma\, b_j\, \beta_j$

$\therefore \quad (a_1\,\alpha_1+a_2\,\alpha_2+\ldots+a_i\,\alpha_i)-(b_1\beta_1+b_2\beta_2+\cdots+b_m\beta_m)=0$

or Linear Combination of L.I. set $S_3=0$

$\therefore$ All the scalars must be zero

i.e. $a_i's=0\ \forall\ i\ b_j's=0\ \forall\ j \Rightarrow \alpha=0$

$\therefore \quad W_1 \cap W_2=\{0\}$

$\therefore \quad V=W_1 \oplus W_2$.

Theorem 16. Existence of supplementary sub space.

Corresponding to each sub space W_1 of a finite dimensional vector space $V(F)$ there exists a sub space W_2 such that V is the direct sum of sub spaces W_1 and W_2

i.e. $V=W_1 \oplus W_2$. **(Meerut 68)**

Another form. *Given an n dimensional vector space V and an m dimensional sub space W_1 then there exists an $n-m$ dimensional sub space W_2 of V such that $V=W_1 \oplus W_2$.*

Proof. Since V is finite dimensional therefore W_1 is also *f.d.* and let

$S_1=\{a_1, a_2, \ldots a_m\}$ be a basis of W_1

then the set S_1 being L.I. can be extended so that the set

$S_2=\{\alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n\}$ $n \geqslant m$ is a basis set for V.

Hence the set $S_3=\{\alpha_{m+1}, \ldots, \alpha_n\}$ consisting of $n-m$ vectors being sub set of L.I. set S_2 is also L.I.

We have to prove the existence of a sub space W_2 so that $V=W_1 \oplus W_2$. *i.e.* $V=W_1+W_2$ and $W_1 \cap W_2=\{0\}$.

Let us choose W_2 to be space generated by S_3 so that $L(S_3)=W_2$. and we shall show the following.

(*a*) W_2 is a sub space (*b*) $V=W_1+W_2$

(*c*) $W_1 \cap W_2=\{0\}$.

(*a*) **W_2 is a sub space.**

Let $\alpha, \beta \in W_2 \Rightarrow \alpha=\Sigma a_i \alpha_i$, $\beta=\Sigma b_i \alpha_i$, $i=m+1, \ldots, n$. as W_2 is spanned by S_2 *i e.* $W_2=L(S_2)$

$$\therefore \quad a\alpha+\beta=a \Sigma a_i \alpha_i+\Sigma b_i \alpha_i=\sum_{i=m+1}^{n}(aa_i+b_i)\alpha_i$$

$=$ L.C. of S_2 and hence $\in W_2$

$\therefore$ W_2 is a sub space.

(*b*) $V=W_1+W_2$

Let $Z \in V \Rightarrow Z=\sum_{i=1}^{n} a_i \alpha_i$ as S_2 is a basis for V.

$$\Rightarrow Z=\sum_{i=1}^{m} a_i \alpha_i \quad +\sum_{i=m+1}^{n} a_i \alpha_i$$

$\Rightarrow Z=$an element of W_1+an element of W_2

$\Rightarrow Z \in W_1+W_2$

$$\therefore \quad V \subset W_1+W_2 \qquad \ldots(1)$$

Again let $Z \in W_1+W_2 \Rightarrow Z=$vector in W_1+vector in W_2

$$\Rightarrow Z=\sum_{i=1}^{m} a_i \alpha_i+\sum_{i=m+1}^{n} a_i \alpha_i=\sum_{i=1}^{n} a_i \alpha_i \Rightarrow Z \in V$$

...(2)

$\therefore \quad W_1+W_2 \subset V$

Hence from 1 and 2 we get

$$V=W_1+W_2$$

(*c*) $W_1 \cap W_2=\{0\}$.

Let $Z\neq 0 \in W_1 \cap W_2 \Rightarrow Z \in W_1$ and $Z \in W_2$.

$$\Rightarrow Z=\sum_{i=1}^{m} a_i \alpha_i = \sum_{g=m+1}^{n} b_g \gamma_g$$

$$\Rightarrow \sum_{i=1}^{m} a_i\alpha_i - \sum_{g=m+1}^{n} b_g \gamma_g=0$$

$\Rightarrow a_i=0 \ \forall i=1,..,m, \quad b_g=0 \ \forall g=m+1,...,n.$

as the set S_2 is a L. I. set being a basis set for V.

$\therefore \quad Z=0$. Hence $W_1 \cap W_2=\{0\}$

From (*a*), (*b*), (*c*) we conclude that W_2 is a sub space of dimension $n-m$ such that $V=W_1 \oplus W_2$. *i.e.* W_2 is a complementary sub space of W_1.

Theorem 17. Dimensions of linear sum.

If W_1, W_2 be two sub spaces of a finite dimensional vector space $V(F)$ then

$$dim\ W_1 + dim\ W_2 = dim\ (W_1+W_2) + dim\ (W_1 \cap W_2)$$

and hence deduce that if

$V=W_1 \oplus W_2$ *then* $dim\ V = dim\ W_1 + dim\ W_2$

(Aligarh 65; Delhi Hon's 69; Kanpur 69; Meerut 67, 70)

Proof. Since V is finite dimensional therefore all its sub spaces W_1, W_2, and $W_1 \cap W_2$ are also *f.d.*

Let $S_1=\{\gamma_1, \gamma_2,...,\gamma_k\}$ be basis of sub space $W_1 \cap W_2$

$\therefore$ dim $(W_1 \cap W_2)=k$ and also S_1 is L. I set. ..(1)

Now $W_1 \cap W_2$ is a sub space of both W_1 and W_2, hence the L.I. set S_1 which is a basis of $W_1 \cap W_2$ can be extended so that the extended sets become basis for W_1 and W_2 respectively.

Let $S_2=\{\gamma_1, \gamma_2,\ldots,\gamma_k, \alpha_1, \alpha_2,\ldots,\alpha_l\}$ be a basis for W_1

$\therefore$ dim $W_1=k+l$. ... (2)

$S_3=\{\gamma_1, \gamma_2, \ldots,\gamma_k, \beta_1, \beta_2, \ldots,\beta_m\}$ be a basis for W_2

$\therefore$ dim $W_2=k+m$. ...(3)

Now we have to prove that

dim W_1 + dim W_2 = dim (W_1+W_2) + dim $(W_1 \cap W_2)$

or $k+l+k+m=\dim (W_1+W_2)+k$

or dim $(W_1+W_2)=k+l+m$. ..(4)

For this we have to search out a L. I. set of $k+l+m$ vectors which spans W_1+W_2 and let this set be

$S_4=\{\gamma_1, \gamma_2, \ldots,\gamma_k, \alpha_1, \alpha_2, \ldots, \alpha_l, \beta_1, \beta_2, \ldots, \beta_m\}$.

Now we shall show that

(*a*) S_4 is L. I. (*b*) $L(S_4)=W_1+W_2$.

(a) For L. I of S_4.

Consider $\sum_{i=1}^{k} c_i \gamma_i+\sum_{j=1}^{l} a_j \alpha_j+\sum_{k=1}^{m} b_k \beta_k=0$. .. (1)

$\therefore \quad \Sigma c_i \gamma_i+\Sigma a_j \alpha_j=-\Sigma b_k \beta_k$.

L. H. S. is L. C. of S_2 which is a basis of W_1 and hence $\in W_1$.

and $-\Sigma b_k \beta_k=-\Sigma b_k \beta_k+\Sigma 0_i \gamma_i$ = L. C. of S_1 which is a basis of W_2 and hence $\in W_2$. But it being equal to L. H. S. therefore belongs to W_1 also.

$\therefore \quad -\Sigma b_k \beta_k \in W_1 \cap W_2$ or $\Sigma b_k \beta_k \in W_1 \cap W_2$ whose basis is S_1.

$\therefore \quad \Sigma b_k \beta_k = L.C.$ of $S_1=\Sigma d_p \gamma_p$.

$\therefore \quad \Sigma b_k \beta_k-\Sigma d_p \gamma_p=0$.

or L. C. of S_3 is a L. I. set $=0$.

$\therefore$ Each of the scalars b_k and d_p for $k=1, \ldots,m$, $p=1,\ldots,k$ are zero.

Since each of b_k is zero the relation (1) reduces to

$$\Sigma c_i \gamma_i+\Sigma a_j \alpha_j=0$$

or L. C. of S_2 is a L. I. set $=\mathbf{0}$.

$\therefore$ Each of scalars c_i and a_j is zero and also b_k are zero as shown above.

Since relation (1) implies that all the scalars are zero therefore the set S_4 is a linearly independent set.

(b) For $\mathbf{L}(S_4)=W_1+W_2$.

Let $Z \in W_1+W_2 \Rightarrow Z=\alpha+\beta,\ \alpha \in W_1,\ \beta \in W_2$

$\Rightarrow$ Z=(1. c. of α^s and β^s of S_2)

$+$(1. c. of β^s and γ^s of S_3)

=(1. c. of α^s, β^s and γ^s of S_4) $\therefore$ $Z \in L(S_4)$.

Hence $W_1+W_2 \subset L(S_4)$. ...(2)

Again let $Z \in L(S_4)$ and proceeding as above in reverse order we can show that $Z \in W_1+W_2$.

$\therefore$ $L(S_4) \subset W_1+W_2$. ...(3)

Hence from (2) and (3) we get $L(S_4)=W_1+W_2$.

Therefore S_4 is a basis set for W_1+W_2 consisting of $k+l+m$ elements.

$\therefore$ dim $(W_1+W_2)=k+l+m=(k+l)+(k+m)-k$

$=$dim W_1+dim W_2-dim $(W_1 \cap W_2)$.

Note. In case $W_1 \cap W_2=\{0\}$ so that dim $(W_1 \cap W_2)=0$ then W_1+W_2 is strengthened to $W_1 \oplus W_2$ and therefore

dim $(W_1 \oplus W_2)=$dim W_1+dim W_2.

§ 14. Quoitent space.

Certain Definitions.

Right and Left Cosets.

Let W be a sub space of vector space $V(F)$ then for any vector $\alpha \in V$ the set

$S_1=\{\alpha+w : w \in W\}$ is called the left coset $\alpha+W$ which is geneated by α and W.

Similarly $S_2=\{w+\alpha : w \in W\}$ is called the right coset $W+\alpha$ which is generated by α and W.

Since $(V, +)$ is an abelian group so is $(W, +)$ and hence by commutative property

$$w+\alpha=\alpha+w \ \forall \ \alpha \in V \text{ and } w \in W.$$

Above relation implies $\alpha+W=W+\alpha$.

In other words it means that the right and left cosets of W become identical and hence we shall denote a coset generated by W and $\alpha \in V$ as

$$W+\alpha=\{w+\alpha : w \in W\}.$$

The set W is a coset by itself.

$$W=\{w : w \in W\}=\{w+0 : w \in W\}=W+0$$

where 0 is the additive identity of V.

Therefore the set W represents the coset W+0 generated by W and 0 ∈ V.

The coset corresponding to α ∈ W is the coset W itself.

$$W+\alpha=\{w+\alpha : w \in W\}.$$

But in this case $\alpha \in W$ $\therefore$ $w+\alpha=w_1 \in W$ as W is a sub space.

$\therefore$ $W+\alpha=\{w_1 : w_1 \in W\}=W$

Hence coset $W+\alpha$=coset W when $\alpha \in W$.

Similarly coset $W+\beta$=coset W when $\beta \in W$.

Thus all the cosets of W with those vectors of V which are also vectors of W are identical with coset W, where as the cosets of W by those elements of V which are not in W are all distinct.

Addition and scalar multiplication of Cosets.

we shall define the addition of cosets as

$$(W+\alpha)+(W+\beta)=W+(\alpha+\beta) : \alpha, \beta \in V \quad ...(1)$$

and scalar multiplication as

$$a\,(W+\alpha)=W+a\alpha \ ; \alpha \in V \text{ and } a \in F. \quad ...(2)$$

whenever $\alpha, \beta \in V$ and $a \in F$ then since V is a vector space we have $\alpha+\beta \in V$ and $a\alpha \in V$ and as such

$W+(\alpha+\beta)$ and $W+a\alpha$ are again cosets.

Hence we conclude that the set of all cosets is closed w. r. t. the operations of coset addition and scalar multiplication of cosets.

Now we shall show that the above operations are well defined *i.e.* they are independent of the particular representation to denote a coset.

Let $W+\alpha=W+\alpha' \Rightarrow W=W+\alpha'+(-\alpha)$ $\alpha, \alpha' \in V$

$\Rightarrow \alpha'-\alpha \in W$. $\because$ $W+\alpha=W$ when $\alpha \in W$.

$\Rightarrow \alpha'=\alpha+w_1$ where $w_1 \in W$ ...(3)

Similarly if $W+\beta=W+\beta'$ then $\beta'=\beta+w_2$ where $w_2 \in W$.

Now $(W+\alpha')+(W+\beta')=W+(\alpha'+\beta')$ by definition

$=W+(\alpha+w_1+\beta+w_2)$ by (3)

$=(W+w_1+w_2)+(\alpha+\beta)$

$=W+(\alpha+\beta)$

$=(W+\alpha)+(W+\beta)$ by (1).

Hence the operation (1) is well defined.

Again $W+\alpha=W+\alpha' \Rightarrow \alpha'-\alpha \in W$ as above

$\Rightarrow a(\alpha'-\alpha) \in W$

$\Rightarrow a\alpha'-a\alpha \in W \Rightarrow W+a\alpha=W+a\alpha'$

$\Rightarrow a(W+\alpha)=a(W+\alpha')$ by (2).

Hence the operation (2) is also will defined.

With the above definitions of addition and scalar multiplication of cosets we are now in a position to give vector space structure to the set of all cosets and this vector space will be called **quotient space** and is denoted by V/W or V'.

Theorem 18. *If W be any sub space of a vector space $V(F)$ then the set V' of all cosets $W+\alpha$, $\alpha \in V$ is a vector space over F for the addition and scalar multiplication of cosets as the two compositions defined as*

$$(W+\alpha)+(W+\beta)=W+(\alpha+\beta),\ \alpha, \beta, \in V \quad ...(1)$$

$$a\ (W+\alpha)=W+a\alpha,\ \alpha \in V,\ a \in F \quad ...(2)$$

and this vector space is called quotient space and is generally denoted by V/W **(Delhi 70)**

Now $V'=\{W+\alpha : \alpha \in V\}$

We have already shown that the set V' is closed both for addition and scalar multiplication and also that the two operations are well defined.

Now we shall verify the postulates of vector space one by one.

1. (V', +) is an abelian group.

(a) Closure property. (Already shown on P. 353)

(b) Associative : $[(W+\alpha)+(W+\beta)]+(W+\gamma)$

$=[W+(\alpha+\beta)]+(W+\gamma)$ by (1)

$=W'+(\alpha+\beta)+\gamma$ by (1) $=W+\alpha+(\beta+\gamma)$

by associativity in V

$=(W+\alpha)+(W'+\beta+\gamma)=(W+\alpha)$

$+[(W+\beta)+(W+\gamma)]$

(c) Identity :

$(W+0)+(W+\alpha)=W+(0+\alpha)=W+\alpha$

$(W+\alpha)+(W+0)=W+(\alpha+0)=W+\alpha.$

$\because$ $\alpha+0=0+\alpha=\alpha$, 0 being the identity in V.

Hence $W+0$ which is a coset in V' is the identity element in V'

(d) Inverse :

$(W+\alpha)+(W'+(-\alpha))=W+\alpha+(-\alpha)=W+0$

$=$Identity

$(W+(-\alpha))+(W+\alpha)=W+((-\alpha)+\alpha)=W+0$

$=$Identity

$\therefore$ $W+(-\alpha)$ is additive inverse of $W+\alpha \in V'$

where $-\alpha$ is additive inverse of $\alpha \in V$.

(e) **Commutative :**

$$(W+\alpha)+(W+\beta)=W+(\alpha+\beta)=W+(\beta+\alpha)$$
$$=(W+\beta)+(W+\alpha)$$
$$\because \quad (V, +) \text{ is abelian group}$$

2. Laws of scalar multiplication.

(a) $a\,(\alpha+\beta)=a\,\alpha+a\,\beta$. $\alpha, \beta \in V$ and $a \in F$

$$a\,[(W+\alpha)+(W+\beta)]=a\,('V+(\alpha+\beta))=W'+a\,(\alpha+\beta)$$
$$=W+a\,\alpha+a\,\beta=(W+a\,\alpha)+(W+a\,\beta)$$
$$=a\,(W+\alpha)+a\,(W+\beta).$$

(b) $(a+b)\,\alpha=a\,\alpha+b\,\alpha$, $a, b \in F$. $\alpha \in V$

$$(a+b)\,[W'+\alpha]=W+(a+b)\,\alpha=W+a\alpha+b\,\alpha$$
$$=(W+a\,\alpha)+(W+b\,\alpha)=a\,(W'+\alpha)$$
$$+b\,(W'+\alpha).$$

(c) $(ab)\,\alpha=a\,(b\,\alpha)$. $a, b \in F$, $\alpha \in V$

$$(ab)\,(W+\alpha)=W+(ab)\,\alpha=W+a\,(b\,\alpha)$$
$$=a\,(W+b\,\alpha)=a\,[b\,(W+\alpha)].$$

(d) $1.\alpha=\alpha$, 1 is the multiplicative identity of F.

$$1.(W+\alpha)=W+1.\alpha=W+\alpha.$$

We have now verified all the postulates of a vector space and hence the set V' or $V'/W=\{W+\alpha : \alpha \in V\}$ is a vector space.

Theorem 19. Dimension of quotient space.

If W be a sub space of a finite dimentional vector space $V(F)$ then dim V/W = dim V − dim W where V/W is the quotient space. **(Delhi Hons 70; Aligarh 65; Meerut; 68, 69) Bombay 70; B. H. U. 68)**

$$V/W=\{W+\alpha : \alpha \in V\}$$

Let dim $V=n$ and dim $W=m$.

Suppose $S_1=\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ is a basis of W then the L. I. set S_1 can be extended to

$$S_2=\{\alpha_1, \alpha_2, \ldots, \alpha_m, \beta_1, \beta_2, \ldots, \beta_t\}.$$

So that the set S_2 consisting of $l+m$ vectors is a basis set for V. $\therefore$ dim $V=l+m=n$ (given).

We have to prove that

dim $V/W=$dim $V-$dim $W=n-m=l+m-m=l$.

For this we have to search out a set of l cosets which should form a basis for V/W.

Consider the set

$$S_3=\{W+\beta_1, W+\beta_2, \ldots, W+\beta_l\}.$$

If S_3 is to be a basis set for V/W then we should prove that

(a) S_3 is a L. I. set, (b) $V/W=L(S_3)$.

(a) S_3 is L. I. set.

Consider $\sum_{i=1}^{l} b_i (W+\beta_i)=0$ of $V/W=W$.

$\Rightarrow W+\sum b_i \beta_i=W$ by addition and scalar multiplication of cosets.

$\Rightarrow \sum b_i \beta_i \in W$ $\because$ $W+\alpha=W$ if $\alpha \in W$.

$\Rightarrow \sum b_i \beta_i=$ l.c. of S_1 which is a basis of W

$\Rightarrow b_i \beta_i=\sum_{j=1}^{m} a_j \alpha_j$

$\Rightarrow \sum b_i \beta_i-\sum a_j \alpha_j=0$.

Above is a l.c. of elements of L. I. set S_2 which is a basis of V.

$\Rightarrow b_i=0$ $i=1,\ldots,l$, $a_j=0$ $j=1,\ldots,m$.

Since $\sum b_i (W+\beta_i)=0$ of $V/W=W \Rightarrow b_i=0 \ \forall \ i$

$\therefore$ the set S_3 is a L. I. set.

(b) $V/W=L(S_3)$.

Let $Z \in V/W \Rightarrow Z=W+\alpha$,

where $\alpha \in V$ whose basis is S_2

$\Rightarrow Z=W+$(l. c. of elements of S_2)

$$\Rightarrow Z=W+(\sum_{j=1}^{m} a_j \alpha_j+\sum_{i=1}^{l} b_i \beta_i).$$

But $\sum_{j=1}^{m} a_j \alpha_j=\alpha$ say $\in W$ as S_1 is a basis set for W.

$$\Rightarrow Z=W+\alpha+\sum_{i=1}^{l} b_i \beta_i \quad \text{where } \alpha \in W$$

$$\Rightarrow Z=W+\sum_{i=1}^{l} b_i \beta_i \quad \because \quad W+\alpha=W \text{ when } \alpha \in W$$

$$\Rightarrow Z=W+(b_1\beta_1+b_2\beta_2+\ldots+b_l\beta_l)$$
$$\Rightarrow Z=(W+b_1\beta_1)+(W+b_2\beta_2)+\ldots+(W+b_l\beta_l)$$
$$\Rightarrow Z=b_1\,(W+\beta_1)+b_2\,(W+\beta_2)+\ldots+b_l\,(W+\beta_l)$$
$$\Rightarrow Z=\text{L. C. of } S_2$$
$$\Rightarrow Z \in L\,(S_3)$$
$$\therefore \quad V/W \subset L\,(S_3).$$

Proceeding in reverse-way we can prove that

$$Z \in L\,(S_3) \Rightarrow Z \in V/W \quad \therefore \quad L\,(S_3) \subset V/W.$$

Hence $V/W=L\,(S_3)$.

$\therefore$ S_3 is a basis set of V/W and since S_3 consists of l elements.

$$\therefore \quad \dim V/W=l=n-m$$
$$=\dim V-\dim W.$$

§ 15. Isomorphism.

Vector space Homomorphism. Linear Transformation.

Definition. *A mapping T of a vector space $U\,(F)$ into a vector space $V\,(F)$ i.e. $T: U \to V$ is called a vector space homomorphism or a linear transformation if T is such that*

(1) $T\,(\alpha+\beta)=T\,(\alpha)+T\,(\beta) \quad \forall\ \alpha, \beta \in V$ **(additive)**

(2) $T(a\alpha)=a\,T(\alpha) \qquad \forall\ \alpha \in U, a \in F$

(Homogeneous)

where $T(\alpha)$ and $T(\beta)$ are the elements of V.

(Delhi 70; Aligarh 65)

Both the above properties 1 and 2 can be combined into single criteria

i.e. $T(c\alpha+\beta)=T(c\alpha)+T(\beta)$ by (1)

or $T(c\alpha+\beta)=cT(\alpha)+T(\beta)$ by (2) $c \in F, \alpha, \beta \in U$.

Above is known as the linearity of T and that is why T is called linear transformation. [L.T.]

§ 16. Properties of homomorphism or L. T. 's.

$f : U(F) \to V(F)$ then,

(a) $f(0)=0'$, *i.e.* the zero vectors of two spaces correspond, the vector zero on the left is additive identity of U and $0'$ on the right is the additive identity of V.

Proof. Let $f(\alpha)=\alpha'$, where $\alpha \in U$ and $\alpha' \in V$.

$\therefore\ f(\alpha+0)=f(\alpha)+f(0)$ by def. $0 \in U$.

$\Rightarrow f(\alpha)=f(\alpha)+f(0)$

$\Rightarrow \alpha'=\alpha'+f(0).\ \alpha' \in V$

$\Rightarrow \alpha'+0'=\alpha'+f(0)$

$f(0)=0'$ by cancellation law.

or

(b) $f(-\alpha)=-f(\alpha), \alpha \in U.$

Let $\alpha \in U \Rightarrow -\alpha \in U$ and $\alpha+(-\alpha)=0$

$\therefore\ f(\alpha+(-\alpha))=f(0) \Rightarrow f(\alpha)+f(-\alpha)=0'$

$\Rightarrow f(-\alpha)$ is additive inverse of $f(\alpha)$ in V

$\Rightarrow f(-\alpha)=-f(\alpha).$

(c) **Kernel of homomorphism.**

$f : U(F) \to V(F).$

The set of all those elements of U whose f images is the

zero of V is called kernel of homomorphism. If this set be denoted by K, then

$$\mathbf{K}=\{\alpha \in U : f(\alpha)=0\}$$

To prove that K is a sub space of U (F) **(Punjab 60)**

Let $\alpha, \beta \in K$, so that $f(\alpha)=0', f(\beta)=0'$.

$$f(a\alpha+b\beta)=f(a\alpha)+f(b\beta)=af(\alpha)+bf(\beta)$$
$$=a.0'+b.0'=0'+0'=0'.$$

Above shows that $a\alpha+b\beta \in K$, when $\alpha, \beta \in K$ and $a, b \in F$.

$\therefore$ K is a sub space of $U(F)$

Illustration.

Let $T : V_3(R) \to V_2(R)$ defined as

$T(a_1, a_2, a_3)=(a_2, a_3) \quad \forall\ a_1, a_2, a_3 \in R$.

We shall show that T defined as above is a homomorphism or a linear transformation. Show further that it is onto and find its kernel

$$T : V_3(R) \to V_2(R).$$

Choose $\alpha=(a_1, a_2, a_3), \beta=(b_1, b_2, b_3) \in V_3(R)$

$\therefore$ $T(\alpha)=(a_2, a_3), T(\beta)=(b_2, b_3)$ by definition ...(1)

then $c\alpha+\beta=c(a_1, a_2, a_3)+(b_1, b_2, b_3), c \in R$

or $(c\alpha+\beta)=(ca_1+b_1, ca_2+b_2, ca_3+b_3)$

$\therefore$ $T(c\alpha+\beta)=(ca_2+b_2, ca_3+b_3)$

$=(ca_2, ca_3)+(b_2, b_3)$

$=c(a_2, a_3)+(b_2, b_3)$

$=c\,T(\alpha)+T(\beta)$ by I.

Since T satisfies the linearity property and hence T is a vector space homomorphism or a linear transformation.

For onto. Let (a_2, a_3) be any element of $V_2(R)$ then there exists an element (a_1, a_2, a_3) in $V_3(R)$ such that

$T(a_1, a_2, a_3)=(a_2, a_3)$. Hence T is onto.

Kernel of T : $W=\{\alpha \in V_3(R) : T(\alpha)=0 \in V_2(R)\}$

where $T(a_1, a_2, a_3)=(a_2, a_3)=(0, 0)$

$\therefore \quad a_2=0, a_3=0$

$\therefore \quad W=\{(a, 0, 0) : a \in R\}$

and by def. $T(a, 0, 0)=(0, 0)$. $\therefore$ W is kernel of T.

§ 17. Vector space Isomorphism.

Definition. *A mapping $T : U \to V$ is called an isomorphism of the vector space $U(F)$ onto the vector space $V(F)$ if*

(1) T is one-one

i.e. $T(\alpha)=T(\beta) \Rightarrow \alpha=\beta$.

(2) T is onto

i.e. for each vector $\alpha' \in V$ $\exists$ a vector α in U such that

$$T(\alpha)=\alpha'.$$

(3) T preserves the two compositions of addition and scalar multiplication

i.e. $T(\alpha+\beta)=T\alpha+T\beta$

$T(a\alpha)=a.T(\alpha)$

Above properties can be stated as under

i.e. T is linear

i.e. $T(c\alpha+\beta)=c\,T(\alpha)+T(\beta)$ $\forall$ $\alpha, \beta \in U$ and $c \in F$.

In this case the two vector spaces $U(F)$ and $V(F)$ are said to be isomorphic and this is symbolically expressed as

$$U(F) \cong V(F).$$

Exercise 5

1. *Let $T : V_2(R) \to V_2(R)$ defined as*

$$T(a_1, b_1)=(b_1, a_1).$$

We shall verify that T is an isomorphism.

(1) **T is one-one.** Let $\alpha=(a_1, b_1,)$ $\beta=(a_2, b_2)$

then $T(\alpha)=T(\beta) \Rightarrow (b_1, a_1)=(b_2, a_2)$ by def. of T

$\Rightarrow b_1=b_2$, and $a_1=a_2 \Rightarrow (a_1, b_1)=(a_2, b_2)$
$\Rightarrow \alpha=\beta$.

Hence T is one-one.

(2) **T is onto.** For every element
$\alpha'=(b_1, a_1) \in V_2(R)$ $\exists$ an element
$\alpha=(a_1, b_1) \in V_2(R)$ such that
$T(\alpha)=\alpha'$ *i e.* $T(a_1, b_1)=(b_1, a_1)$.

Hence T is onto.

(3) **T is linear.** $c\alpha+\beta=c(a_1, b_1)+(a_2, b_2)$
$=(ca_1+a_2, cb_1+b_2)$

$\therefore$ $T(c\alpha+\beta)=(cb_1+b_2, ca_1+a_2)$ by def. of T
$=(cb_1, ca_1)+(b_2, a_2)$
$=c(b_1, a_1)+(b_2, a_2)$
$=c\ T(\alpha)+T(\beta)$

Hence T is linear.

Therefore T is an isomorphism

2. *Let $V(R)$ be the vector spuce of all complex numbers $a+ib$ over the field of reals and T be a mapping from $V(R)$ to $V_2(R)$ defined as*

$$T(a+ib)=(a, b). \qquad \ldots(1)$$

We shall verify that T is an isomorphism.

T is one-one. Let $\alpha=a+ib$, $\beta=c+id$, $\alpha, \beta \in V(R)$
$T(\alpha)=T(\beta) \Rightarrow (a, b)=(c, d)$ by def of T
$\Rightarrow a=c, b=d \Rightarrow a+ib=c+id$
$\Rightarrow \alpha=\beta$.

Hence T is one-one.

T is onto. For each
$(a, b) \in V_2(R)$ $\exists$ a vector $a+ib \in V(R)$
s.t. $T(a+ib)=(a, b)$.

Hence T is onto,

T is linear. $k\alpha+\beta=k(a+ib)+(c+id)$

$=(ka+c)+i(kb+d)$

$T(k\alpha+\beta)=(ka+c, kb+d)$ by def. of T.

$=(ka, kb)+(c, d)=k(a, b)+(c, d)$

$=k\,T(a+ib)+T(c+id)$

$=k\,T(\alpha)+T(\beta)$.

Hence T is linear.

Hence T defined as in I is an isomorphism.

3. *Let* $T_a : R^3 \to R^3$ *defined as*

$T_a(x, y, z)=(x, y, az)$, $a\neq 0$, *where a is fixed in R.*

Show that T_a *is an isomorphism of* R^3 (R) *onto itself.*

Let $\alpha=(x_1, y_1, z_1)$, $\beta=(x_2, y_2, z_2)$

$\therefore\quad c\alpha+\beta=(cx_1+x_2, cy_1+y_2, cz_1+z_2)$

$\therefore\quad T_a(c\alpha+\beta)=\{cx_1+x_2, cy_1+y_2, a(cz_1+z_2)\}$

$=c(x_1, y_1, az_1)+(x_2, y_2, az_2)$.

$=c\,T_a\,\alpha+T_a\,\beta$ by def. of T_a.

$\therefore$ **T_a is linear.**

T is one-one $T_a\,\alpha=T_a\,\beta$

$\Rightarrow (x_1, y_1, az_1)=(x_2, y_2, az_2)$

$\Rightarrow x_1=x_2, y_1=y_2, az_1=az_2$.

Since $a\neq 0$. $\quad\therefore\quad z_1=z_2$.

Hence $\alpha=\beta$.

$\therefore$ T_a is one one.

T is onto. For every vector $(x, y, z) \in R^3$ the range, $\exists$ a vector, $\left(x, y, \frac{1}{a}z\right) \in R^3$ the domain *s.t.*

$$T_a\left(x, y, \frac{1}{a}z\right)=\left(x, y, a.\frac{1}{a}z\right)=(x, y, z).$$

Hence T is onto and therefore T is an isomorphism.

Theorem 20. (V. Imp.)

Every n dimensional vector space $V(F)$ *is isomorphic to* $V_n(F)$ *i.e.* F^n **(Aligarh 65, Meerut 69)**

Since $V(F)$ is of dimension n as such it has a basis set $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ consisting of n elements and every vector α in $V(F)$ is uniquely expressible as a l.c. of the elements of the basis set

$$i.e.\ \alpha = a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n = \Sigma\, a_i\, \alpha_i \qquad \ldots(1)$$

where $a_1, a_2, \ldots, a_n \in F$

The elements of $V_n(F)$ are ordered n-tuples and as such the n-tuple $(a_1, a_2, \ldots, a_n) \in V_n(F)$. In order to prove that $V(F) \cong V_n(F)$ we have to show the existence of a one-one onto, linear transformation.

$$T : V(F) \to V_n(F) \text{ which we define as under.}$$

$$T(\alpha) = (a_1, a_2, \ldots, a_n\}. \qquad \ldots(2)$$

As the scalars a_i's in (V) are unique therefore $T(\alpha)$ given by (2) is a unique element of $V_n(F)$ and hence T is well defined.

T is one-one. Let $\beta = \Sigma\ b_i\alpha_i$

Now $T(\alpha) = T(\beta) \Rightarrow (a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$

$$\Rightarrow a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n.$$

$\therefore\ \Sigma\, a_i\alpha_i = \Sigma\, b_i\alpha_i$ or $\alpha = \beta$. Hence T is one-one

T is onto. For this we have to show that corresponding to each n-tuple say

$(c_1, c_2, \ldots, c_n) \in V_n(F)\ \exists$ a vector γ in $V(F)$

s.t. $T(\gamma) = (c_1, c_2, \ldots, c_n)$

Let $\gamma = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n$ in terms of basis set

$\therefore\ T(\gamma) = (c_1, c_2, \ldots, c_n)$ by def. of T, and it proves the existence of γ. Hence T is onto.

T is linear. $\alpha = \Sigma\ a_i\alpha_i,\ \beta = \Sigma\ b_i\alpha_i$

$\therefore \quad c\alpha+\beta=\Sigma\,(ca_i+b_i)\alpha_i$ and it belongs to $V\,(F)$

$\therefore \quad T\,(c\alpha+\beta)=(ca_1+b_1,\ ca_2+b_2,\ldots,ca_n+b_n)$ by def.

$=(ca_1,\ ca_2,\ldots,ca_n)+(b_1,\ b_2,\ldots,b_n)$

$=c\,(a_1,\ a_2,\ldots,a_n)+(b_1,\ b_2,\ldots,b_n)$

$=c\,T\,(\alpha)+T\,(\beta)$ by def.

Hence T is linear and therefore

$$V\,(F)\cong V_n\,(F)$$

Theorem 21. *Two finite dimensional vector spaces $U\,(F)$ and $V\,(F)$ are isomorphic if and only if dim U=dim V.* **(Meerut M.Sc. 68)**

Case I. Given that $U\,(F)\cong V(F)\Rightarrow \exists$ a one-one-onto linear mapping

$$T: U\,(F)\to V\,(F)$$

we shall prove that dim U=dim V.

Let us suppose that dim $U=n$, so that by definition there exists a basis set $A=\{\alpha_1,\ \alpha_2,\ldots,\alpha_n\}$ consisting of n elements. We shall now establish that the set

$$B=\{T(\alpha_1),\ T(\alpha_2),\ldots,T(\alpha_n)\}$$

consisting of n vectors belonging to V is a basis set of V. In order to prove that B is a basis set of V we have to establish that the set B is linearly independent and it spans V.

i.e. $L(B)=V$.

The set B is linearly independent.

Consider $a_1\,T\,(\alpha_1)+a_2\,T\,(\alpha_2)+\ldots+a_n\,T\,(\alpha_n)=0'\in V$.

.. (1)

or $T(a_1\alpha_1)+T\,(a_2\alpha_2)+\ldots+T\,(a_n\alpha_n)=T\,(0)\ 0\in U$

$\because \quad T(a\alpha)=a\,T\,(\alpha)$ and $T\,(0)=0'$ as T is a L.T.

or $T\,(a_1\alpha_1+a_2\alpha_2+\ldots+a_n\,\alpha_n)=T\,(0)$

$\because \quad T\,(\alpha+\beta)=T\,(\alpha)+T\,(\beta)$ as T is a L.T.

$\therefore \quad a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n=0$

.. (2)

$\because$ T is one-one which means that

$$T(\alpha)=T(\beta) \Rightarrow \alpha=\beta.$$

But since $\{\alpha_1, \alpha_2,\ldots,\alpha_n\}$ is a basis set and as such it is L.I. and by definition of L.I. we must have

$$a_1=0,\ a_2=0,\ldots,a_n=0 \text{ from (2)}$$

and hence from I we conclude that the set

$$T(\alpha_1),\ T(\alpha_2),\ldots,T(\alpha_n) \text{ is also L.I. set.}$$

The set B spans V.

Let $\alpha \in U$ and $\beta \in V$ and since T is onto therefore we have

$$T(\alpha)=\beta \qquad \ldots(3)$$

or $T(a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n)=\beta$ as A is a basis set for U.

or $a_1\ T(\alpha_1)+a_2\ T(\alpha_2)+\ldots+a_n\ T(\alpha_n)=\beta$ by Linearity of T.

Hence a vector $\beta \in V$ has been expressed as a linear combination of vectors $T(\alpha_1),\ T(\alpha_2),\ldots,T(\alpha_n)$ of the set B and therefore the set B spans V.

$\therefore$ B is a L.I. set of n vectors which spans V and as such it is a basis set $\therefore$ dim $V=n=$dim U.

Another form.

Cor. *Prove that the image set of a basis set under an isomorphism is a basis set*

We have already proved it in the above

Converse. Given. dim U=dim V=n say.

To prove that U$\cong$V *i.e.* $\exists$ a linear transformation $T: U \to V$ which is one-one and onto as well

Let $A=\{\alpha_1, \alpha_2,\ldots,\alpha_n\}$, $B=\{\beta_1, \beta_2,\ldots,\beta_n\}$ be the basis sets consisting of n elements each for U and V respectively

$\therefore$ $\alpha \in U \Rightarrow \alpha=\Sigma\ x_i\alpha_i$ as A is a basis set of U.

Now let us define a mapping $T: U \to V$ such that $T(\alpha)=T(\Sigma\ x_i\alpha_i)=\beta=\Sigma\ x_i\beta_i$ as B is a basis set of V.

We have chosen the same scalars x_i for expressing α and β as l.c. of their respective basis.

We shall establish that T defined as above is an isomorphism. From definition (1) we conclude that if α_i is a member of basis set A then

$$T(\alpha_i)=T(0\alpha_1+0\alpha_2+\ldots+1.\alpha_i+\ldots+0\alpha_n)$$
$$=0\beta_1+0\beta_2+\ldots+1.\beta_i+\ldots+0\beta_n)=\beta_i$$

by def. of T choosing same scalars.

i.e. $T(\alpha_i)=\beta_i$ for each i

T is Linear.

Let $\alpha=\Sigma x_i\alpha_i$, $\gamma=\Sigma y_i\alpha_i \in U$. so that

$c\alpha+\gamma=\Sigma(cx_i+y_i)\alpha_i \in U$

$\therefore$ $T(c\alpha+\gamma)=\Sigma(cx_i+y_i)\beta_i$ by def. of T

Also $c\,T(\alpha)+T(\gamma)=c\,\Sigma x_i\beta_i+\Sigma y_i\beta_i$ by def. of T

$$=\Sigma(cx_i+y_i)\beta_i$$

$\therefore$ $T(c\alpha+\gamma)=cT(\alpha)+T(\gamma)$. Hence T is linear.

T is one-one.

Let $T(\alpha)=T(\gamma)$ where $\alpha\ \gamma \in U$.

$\therefore$ $T(\Sigma x_i\alpha_i)=T(\Sigma y_i\alpha_i)$

$\Rightarrow \Sigma x_i\beta_i=\Sigma y_i\beta_i$ by def. of T

$\Rightarrow \Sigma(x_i-y_i)\beta_i=0\ \forall\ i$

$\Rightarrow x_i-y_i=0\ \forall\ i$ as basis set B is L.I.

$\Rightarrow x_i=y_i\ \forall\ i$

$\Rightarrow \Sigma x_i\alpha_i=\Sigma y_i\alpha_i \Rightarrow \alpha=\gamma$

Hence T is one-one

T is onto. Let $\beta=\sum_{i=1}^{n} x_i\beta_i$ be a vector in V, then by definition of T the vector $\Sigma x_i\alpha_i=\alpha$ say which is in U is such that $T(\alpha)=\beta$. Hence T is **onto.**

$\therefore$ $U \cong V$.

Exercise 6

Ex. 1. *If V and W are two finite dimensional vector spaces such that dim V=dim W and f is an isomorphism of V into W, prove that f must map V onto W.*

Let dim $V=n$ and $f: V\to W$ be an isomorphism of V into W which means that f is both linear and one-one but not onto, we have to prove that f is onto also.

Let $A=\{\alpha_1,\alpha_2, \ldots, \alpha_n\}$ be a basis of V of dim n,
then $B=\{T\alpha_1, T\alpha_2, \ldots, T\alpha_n\}$ is a L.I. set as shown on *P.* 364

Since B is a L.I. set of n vectors of finite dimensional vector space V therefore it should be a basis for W whose dimension is also n. Hence any vector $\alpha \in W$ is expressible as a linear combination of elements of B.

f is onto : Let $B \in W$ then as shown above

$$\beta = \text{l.c. of } B = (a_1 f\alpha_1 + a_2 f\alpha_2 + \ldots + a_n f\alpha_n)$$

or $$\beta = f(a_1\alpha_1) + f(a_2\alpha_2) + \ldots + f(a_n\alpha_n)$$

$$= f(a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n)$$

$$= f(\alpha) \quad \text{as } A \text{ is basis for } V$$

thus for every $\beta \in W \exists\ \alpha$ in V such that $f(\alpha)=\beta$ and hence f is onto and consequently f is isomorphism.

Deduction.

We can in a similar manner prove that if V is finite dimensional vector space of dim n and f is an isomorphism of V into V, prove that f must map V onto V

Ex. 2. *If V is finite dimensional and f is a homomorphism of V* **onto** *V prove that f must be one-one and so an isomorphism.*

Given V is finite dimensional say of dimension n as such it has a basis set

$S=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ consisting of n L.I. vectors

$f: V\to V$ and f is a homomorphism which is onto

Hence any vector $\alpha \in V$ is the f image of some vector

$$\beta \in V$$

$\therefore\ \alpha = f(\beta) = f(a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n)$ $\because$ S is basis of V

$\therefore\ \alpha = a_1 f(\alpha_1) + a_2 f(\alpha_2) + \ldots + a_n f(\alpha_n)$

$\therefore\ \alpha \in V$ = expressible as a l.c. of elements of S' where

$S = \{f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)\}$ *i e. a* set of n vectors.

$\therefore\ V \subset L(S')$. Also $L(S') \subset V$

$\therefore\ V = L(S')$.

Now V is a finite dimensional vector space of dimension n and S' is a set consisting of n vectors of V such that $L(S') = V$, it follows that S' must be a basis of V. Hence S' is linearly independent.

In order to prove f to be an isomorphism we have only to prove that f is one-one as it is given that f is homomorphism *i.e.* linear, and onto.

f will be one-one if

$$f(\alpha) = f(\beta) \Rightarrow \alpha = \beta$$

Now $\alpha = \Sigma\, a_i\alpha_i \qquad \beta = \Sigma\, b_i\alpha_i$ as S is a basis

$\therefore\ f(\alpha) = f(\beta) \Rightarrow f(\Sigma\, a_i\alpha_i) = f(\Sigma\, b_i\alpha_i)$

$\Rightarrow \Sigma\, a_i f(\alpha_i) = \Sigma\, b_i f(\alpha_i)$ as f is linear

$\Rightarrow \Sigma\, (a_i - b_i) f(\alpha_i) = 0$

$\Rightarrow a_i - b_i = 0\ \ \forall\ i$ as S' is L.I. set

$\Rightarrow a_i = b_i\ \ \forall\ i \Rightarrow \alpha = \beta$.

Since $f(\alpha) = f(\beta) \Rightarrow \alpha = \beta$ is follows that f is one-one and hence f is an isomorphism.

Ex. 3. *If V is finite dimensional and f is a homomorphism of V into itself which is not onto prove that there is some $\alpha \neq 0$ in V such that $f(\alpha) = 0$*

We know that if f be a homomorphism then $f(0) = 0$

Let us suppose that there is no non-zero α in V such that $f(\alpha) = 0$

It means that f is one-one because

$$f(\beta)=f(\gamma) \Rightarrow f(\beta)-f(\gamma)=0$$
$$\Rightarrow f(\beta-\gamma)=0 \qquad \text{as } f \text{ is linear}$$
$$\Rightarrow \beta-\gamma=0 \qquad \text{by supposition}$$
$$\Rightarrow \beta=\gamma$$

Hence f is one-one.

Now V is finite dimensional and f is homomorphism which is one-one and hence f must be onto. We are given that f is not onto. Hence our supposition that there is no non-zero α such that $f(\alpha)=0$ is wrong. In other words there is some $\alpha \neq 0$ such that $f(\alpha)=0$.

Ex. 4. If $A=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *is a basis of* V *over* F *and if* $B=\{\beta_1, \beta_2, \ldots, \beta_n\}$ *in* V *are linearly independent over* F *then show that* $m \leqslant n$. *Hence show that* $F^n \cong F^m$ *if* $n=m$ *where* F^n *is the totality of all ordered n-tuples over the field F.* **(Delhi 70; Meerut 70)**

The basis set A contains n vectors so that dim $V=n$ also we know from Cor. P. 343 that any set of $(n+1)$ or more vectors in an $n-$dimensional vector space is L.D.

Hence $m \leqslant n$.

Again from theorem 20 P. 363 we know that $V \simeq F^n$ where dim $V=n$ ...(1)

Also if W be a sub space of V of dim. m then

$$W \cong F^m \qquad \ldots(2)$$

Iso rom Theorem 21 P. 364

$$V \cong W \Leftrightarrow \dim V=\dim W \qquad \ldots(3)$$

Hence $F^n \simeq F^m$ iff $n=m$. From 1, 2 and 3.

Theorem 22. *Let* U *be a f d. V.S. over the field* F *and the set* $A=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *is a basis of* U. *Let* V *be a vector space over the same field* F *and let* $B=\{\beta_1, \beta_2, \ldots, \beta_n\}$ *be a basis*

of V. Then there exists a unique linear transformation T from U into V such that

$$T\alpha_j=\beta_j \quad j=1, 2,...,n.$$

Let $\alpha \in U \therefore \alpha=\Sigma x_i \alpha_i=x_1\alpha_1+x_2\alpha_2+...+x_n\alpha_n.$

Let us define $T : U \to V$ such that

$T(\alpha)=\Sigma x_i\beta_i=x_1\beta_1+x_2\beta_2+...+x_n\beta_n \in V$ as B is a basis for V

From above definition we conclude that

$$\alpha_i=0\alpha_1+0\alpha +...+1.\alpha_i+...+0\alpha_n$$

$\therefore T(\alpha_i)=0\beta_1+0\beta_2+...+1.\beta_i+...+0\alpha_n=\beta_i$ by def. of T.

Also T is Linear.

Let $\alpha=\Sigma x_i\alpha_i, \gamma=\Sigma y_i\alpha_i \in U$ so that

$c\alpha+\gamma=\Sigma (cx_i+y_i)\alpha_i$

$\therefore T(c\alpha+\gamma)=\Sigma (cx_i+y_i)\beta_i$ by def. of T

Also $c\,T(\alpha)+T(\gamma)=c\,\Sigma x_i\beta_i+\Sigma y_i\beta_i$ by def. of T

$=\Sigma (cx_i+y_i)\beta_i=T(c\alpha+\gamma)$

Hence T is linear

Uniqueness of T.

Let T' be any other linear transformation from $U \to V$ so that $T'\alpha_j=\beta_j \quad \forall\, i$

then $\alpha=\Sigma x_i\alpha_i \quad \therefore \quad T'(\alpha)=T'(\Sigma x_i\alpha_i)$

$=\Sigma x_i\, T'(\alpha_i)$ by linearity of T'

or $T'(\alpha)=\Sigma x_i\beta_i=T(\alpha) \ \forall\ \alpha,$

Hence $T=T'$

Theorem 23. *If W_1 and W_2 are complementary sub spaces of vector space $V(F)$ then the mapping $T : W_2 \to V/W_1$ which assigns to each vector $\beta \in W_2$ the coset $W_1+\beta \in V/W_1$ i.e. $T(\beta)=W_1+\beta$. is an isomorphism.* **(Meerut 69)**

Since W_1 and W_2 are complementary sub spaces hence

$$W_1 \cap W_2=\{0\}. \qquad ...(1)$$

T is one-one. Let β_1 and $\beta_2 \in W_2$ then $\beta_1-\beta_2$ also $\in W_2$
$T(\beta_1)=T(\beta_2) \Rightarrow W_1+\beta_1=W_1+\beta_2$ by def. of T.
$\Rightarrow W_1+(\beta_1-\beta_2)=W_1$
$\Rightarrow \beta_1-\beta_2 \in W_1 \quad \because \quad W_1+\alpha=W_1$ when $\alpha \in W_1$.
But $\beta_1-\beta_2 \in W_2$ also and therefore $\beta_1-\beta_2 \in W_1 \cap W_2$.
But by (1) $W_1 \cap W_2=\{0\}$
$\therefore \quad \beta_1-\beta_2=0$ and hence $\beta_1=\beta_2$
$\therefore \quad T(\beta_1)=T(\beta_2) \Rightarrow \beta_1=\beta_2$
$\therefore \quad T$ is one-one

T is onto. Let the coset $W_1+\gamma \in V/W_2$ then we have to show that $\exists$ a vector $\beta \in W_2$ whose T image is the coset $W_1+\gamma$ *i.e.* $T(\beta)=W_1+\gamma$.

$W_1+\gamma \in V/W_1$ when $\gamma \in W_2$
Since $\gamma \in W_2 \Rightarrow \gamma \in V \Rightarrow \gamma=\alpha+\beta$, $\alpha \in W_1$, $\beta \in W_2$ as W_1 and W_2 are complementary sub spaces *i.e.*

$$V=W_1 \oplus W_2$$

$$\therefore \quad W_1+\gamma=W_1+(\alpha+\beta)=(W_1+\alpha)+(W_1+\beta)$$
$$=W_1+(W_1+\beta) \quad \because \quad W_1+\alpha=W_1 \text{ as } \alpha \in W_1$$
$$=W_1+\beta=T(\beta) \text{ by def. of } T$$

Thus for each coset
$W_1+\gamma \in V/W_1$ $\exists$ a vector $\beta \in W_2$ s t.
$T(\beta)=W_1+\gamma$ and hence T is onto.

T is linear. Let β_1 and $\beta_2 \in W_2$ so that $c\beta_1+\beta_2$ also $\in W_2$ which is a sub space, then
$T(c\beta_1+\beta_2)=W_1+(c\beta_1+\beta_2)$ by def. of T.
$=(W_1+c\beta_1)+(W_1+\beta_2)$ by addition of cosets
$=c(W_1+\beta_1)+(W_1+\beta_2)$ by scalar mult. of cosets
$=c\,T(\beta_1)+T(\beta_2)$ by def. of T.

Hence T is linear.

Since $T: W_2 \to V/W_1$ satisfies all the properties of isomorphism and as such it is an isomorphism.

§ 18. LINEAR TRANSFORMATIONS

Definitions. Linear Transformation.

(*a*) *Let $V(F)$ and $W(F)$ be two vector spaces over the same field F. A function $T: V \to W$ is called a* **linear transformation (or vector space homomorphism)** *from V into W if it satisfies the following properties*

(*1*) $T(\alpha+\beta)=T\alpha+T\beta$. $\forall\ \alpha, \beta \in V$.

i.e. T carries the sum of two vectors of V to the sum of the T images of the vectors. **This is known as additive property of T.**

(*2*) $T(a\alpha)=aT\alpha$. $\forall\ \alpha \in V$ *and* $a \in F$

i.e. T carries the scalar multiple of a vector $\alpha \in V$ *to the same scalar multiplication of the T image of that vector* **This is known as homogeneous property of T.**

Above shows that T preserves the vector space compositions of addition and scalar multiplication.

Both the above properties could be combined into one as under.

$$\mathbf{T}(\mathbf{c}\,\alpha+\beta)=T(c\alpha)+T(\beta)=\mathbf{c}\,\mathbf{T}(\alpha)+\mathbf{T}(\beta)$$

This is known as linearity of T. We shall use this single criteria instead of satisfying the first two properties given above.

( ) **Linear operator on V.**

If in the above definition (*a*) the vector space W is the same as V then the linear transformation $T: V \to V$ is called a linear operator such that

$$T(c\,\alpha+\beta)=c\,T(\alpha)+T(\beta).$$

$$\forall\ \alpha, \beta \in V,\ c \in$$

Thus a linear operator is a function or mapping from V into itself. Whenever it is referred that T is a linear transformation on V it would mean that T is a linear operator.

(c) Linear Functional on V.

Again if T be a mapping from vector space V (F) to its field F

i.e. $T : V \to F$ s.t. $T(c\alpha+\beta)=c\ T(\alpha)+T(\beta)$

$\forall\ \alpha, \beta \in V, c \in F$

Then T is called a linear functional on V.

(d) Identity Transformation I on V

i.e. (Identity operator)

If $I(\alpha)=\alpha \quad \forall\ \alpha \in V$

then I is called identity transformation on V.

I is linear.

Let $\alpha, \beta \in V$ and $c \in F$

then $c\alpha+\beta \in V$ which is a $V.S.$

$\therefore \quad I(c\alpha+\beta)=c\alpha+\beta$ by def. of I

$=c\ I(\alpha)+I(\beta)$

$\because \quad I\alpha=\alpha$ and $I\beta=\beta$

Hence I is linear.

(e) Zero transformation O on V.

If $\mathbf{O}(\alpha)=\mathbf{0} \in V \ \forall\ \alpha \in V$

then **O** is called zero transformation on V.

O transformation is linear

Let $\alpha, \beta \in V$ and $c \in F$ so that

$c\alpha+\beta \in V$ as V is *a* $V.S.$

$\therefore \quad \mathbf{O}(c\alpha+\beta)=\mathbf{0}$ by definition of zero transformation

$=\mathbf{0}+\mathbf{0}$ as **0** is the additive identity of V.

$\therefore \quad =c\mathbf{0}+\mathbf{0}$ as in *a* V. S. $c\mathbf{0}=\mathbf{0}$

$=c\ \mathbf{O}(\alpha)+\mathbf{O}(\beta)$

$\because \quad \mathbf{O}(\alpha)=\mathbf{0}, \mathbf{O}(\beta)=\mathbf{0}$

Hence $\mathbf{O} : V \to V$ is a linear transformatlon (operator).

on V

Zero functional.

If $\mathbf{O}(\alpha)=0 \in F\ \forall\ \alpha \in V.$

then **O** is said to be a zero functional.

Zero transformation from V(F) to W (F).

If $\mathbf{O}(\alpha)=0' \in W, \forall \alpha \in V$.

then **O** is called zero transformation from V to W.

Hence $T: V \to V$ such that $T(\alpha)=0 \in V \forall \alpha \in V$

then $T=\mathbf{O}$ *i.e.* zero operator

$T: V \to F$ such that $T(\alpha)=0 \in F \forall \alpha \in V$

then $T=\mathbf{O}$ *i.e.* zero functional

$T: V \to W$ such that $T(\alpha)=0' \in W \forall \alpha \in V$

then $T=\mathbf{O}$ *i.e.* zero transformation.

Note. If $T: V \to W$ then we shall denote the additive identities of V and W by 0 and 0' respectively 0 will stand for zero of field. **O** will stand for zero operator, functional or transformation as the case may be

(*f*) Addition of linear transformations.

Let T_1 and T_2 be linear transformations on V into W then sum of two linear transformations is defined as

$(\mathbf{T_1}+\mathbf{T_2})\,\alpha=\mathbf{T_1}\,\alpha+\mathbf{T_2}\,\alpha \;\forall\; \alpha \in V$

i.e. T_1+T_2 is a mapping which carries any element $\alpha \in V$ to the sum of its T_1 and T_2 images in W.

To prove that $\mathbf{T_1}+\mathbf{T_2}$ is linear.

Let $\alpha, \beta \in V$ and $c \in F$ so that $c\alpha+\beta \in V$

then $(T_1+T_2)(c\alpha+\beta)$

$=T_1(c\alpha+\beta)+T_2(c\alpha+\beta)$ by def. of T_1+T_2

$=(c\,T_1\alpha+T_1\,\beta)+(c\,T_2\alpha+T_2\beta)$ as T_1 and T_2 are L.T.'s

$=c\,[T_1\alpha+T_2\alpha]+[T_1\beta+T_2\beta)$

$=c\,[(T_1+T_2)\,\alpha]+(T_1+T_2)\,\beta$. by def. of T_1+T_2.

Hence T_1+T_2 is linear.

(*g*) Scalar multiplication of a linear transformation.

Let T be a linear transformation from V into W and a be a scalar $\in F$, then the mapping $a\,T$ is defined as

$(aT)\ \alpha = a\ [T\ (\alpha)]$, $\forall\ \alpha \in V$ and $a \in F$.

i e. aT carries an element $\alpha \in V$ to the same scalar multiple of T image of α.

To prove that aT is linear.

Let $\alpha, \beta \in V$ and $c \in F$ then $c\alpha+\beta \in V$,

$$(aT)\ (c\alpha+\beta) = a\ [T\ (c\alpha+\beta)] \text{ by def. of } aT$$
$$= a\ [cT\ (\alpha)+T\beta] \text{ as } T \text{ is linear}$$
$$= c\ aT\ (\alpha)+a\ T(\beta)$$
$$= c\ (aT)\ \alpha+(aT)\ \beta \text{ by def. of } aT.$$

Hence aT is linear.

(*h*) **Additive inverse of a linear transformation.**

The mapping $-T$ defined as $(-T)\ \alpha = -[T\ (\alpha)]$ is called the additive inverse of linear transformation T.

To prove that —T is linear.

Let $\alpha, \beta \in V$ and $c \in F$ so that $c\alpha+\beta \in V$

$$\therefore\ (-T)\ (c\alpha+\beta) = -[T\ (c\alpha+\beta)]$$
$$= -[c\ T\ (\alpha)+T\ (\beta)] \text{ as } T \text{ is linear}$$
$$= c\ [-T\ (\alpha)]+[-T\ (\beta)]$$
$$= c\ (-T)\ \alpha+(-T)\ \beta \text{ by def. of } -T.$$

Hence $-T$ is linear.

Cor. $T\ (-\alpha) = -T\ (\alpha)\ \forall\ \alpha \in V$

$$T\ (-\alpha) = T\ [(-1)\ \alpha]$$
$$= (-1)\ T\ \alpha = -T\alpha \quad \because \quad T\ (a\alpha) = a\ T\ (\alpha)$$

$$T\ (\alpha-\beta) = T\ [(\alpha+(-\beta)]$$
$$= T\ (\alpha)+T\ (-\beta) \text{ by linearity of } T$$
$$= T\ (\alpha)-T\ (\beta).$$

(*i*) **If T : V→W then zero vectors of V and W correspond.**

i.e. T carries zero vector $\mathbf{0}$ of V to zero vector $\mathbf{0}'$ of W.

Let $\alpha \in V$ so that $T\ (\alpha) = \alpha'$ say $\in W$

Now $\alpha+\mathbf{0} = \alpha$ where $\mathbf{0} \in V$

then $T\ (\alpha) = T\ (\alpha+\mathbf{0}) = T(\alpha)+T\ (\mathbf{0})$

or $\alpha' = \alpha'+T\ (\mathbf{0})$ where $\alpha' \in W$.

Above shows that $T(0)$ is the zero vector of W.

i.e. $T(0)=0'$

where 0 and 0′ are the additive identities of V and W respectively.

(j) Vector space isomorphism.

If T be a mapping from $V(F)$ to $W(F)$ such that

(1) T is one-one.

(2) T is onto.

(3) T preserves the vector space compositions which in other words means that

$$T(c\alpha+\beta)=cT(\alpha)+T(\beta) \ \forall\ \alpha, \beta \in V \text{ and } c \in F$$

then the two vector spaces $V(F)$ and $W(F)$ are said to isomorphic and expressed as $V \cong W$.

Theorem 24. Vector space of linear transformations.

Prove that the set of all linear transformations from $V(F)$ to $W(F)$, denoted by $L(V, W)$ forms a vector space over the field F with respect to addition and scalar multiplication of linear transformations as defined in (f) and (g).

(Kanpur 69, Meerut 68, 69)

We shall now verify that the set $L(V, W)$ satisfies all the axioms of a vector space.

L (V, W) is an additive abelian group.

Let $T_1, T_2, T_3 \in L(V, W)$ then

(1) **Closure.** The sum of two linear transformations is again a L.T. as shown in (*f*) [Reproduce here]

(ii) **Associative.** $(T_1+T_2)+T_3=T_1+(T_2+T_3)$,

$$[(T_1+T_2)+T_3]\,\alpha=(T_1+T_2)\alpha+T_3(\alpha) \quad \text{by def. of } T_1+T_2$$
$$=[T_1(\alpha)+T_2(\alpha)]+T_3(\alpha)$$

But $T_1(\alpha)$, $T_2(\alpha)$, $T_3(\alpha)$ are all elements of W which is a vector space in which addition is associative.

$$=T_1(\alpha)+[T_2(\alpha)+T_3(\alpha)]$$
$$=T_1(\alpha)+[(T_2+T_3)\,\alpha]=[T_1+(T_2+T_3)]\,\alpha$$

or $[(T_1+T_2)+T_3]\alpha=[T_1+(T_2+T_3)]\alpha. \quad \forall\ \alpha \in V.$

$\therefore \quad (T_1+T_2)+T_3=T_1+(T_2+T_3)$

(iii) Identity. zero transformation is the identity element of $L(V, W)$.

$\because \quad (T+\mathbf{O})\ \alpha=T(\alpha)+\mathbf{O}(\alpha)=T(\alpha)+\mathbf{0}'=T(\alpha).$

$\therefore \quad T+\mathbf{O}=T. \quad \forall\ T \in L(V, W)$

Similarly $\mathbf{O}+T=T.$

(iv) **Inverse.** The inverse of any transformation

$$T \in L(V, W)$$

is $-T$, where $(-T)\ \alpha=-[T(\alpha)]$ by def.

Now $[T+(-T)]\ \alpha=T(\alpha)+(-T)\ \alpha=T(\alpha)-T(\alpha).$

$$=\mathbf{0}'=\mathbf{O}(\alpha)$$

$\therefore \quad T+(-T)=\mathbf{O}$ *i.e.* identity.

Hence the inverse of every transformation T exists which is $-T$ and which is *a* L.T. as shwon in (*h*) P. 376

(v) **Commutative.** *i.e.* $T_1+T_2=T_2+T_1.$

$(T_1+T_2)\ \alpha=T_1(\alpha)+T_2(\alpha)$

But $T_1(\alpha)$ and $T_2(\alpha)$ are elements of vector space W in which addition is commutative and hence it can be written as

$$=T_2(\alpha)+T_1(\alpha)=(T_2+T_1)\ \alpha,$$

Hence $T_1+T_2=T_2+T_1.$

Thus $L(V, W)$ is an additive abelian group :

Laws of scalar multiplication.

For any vector space V the following laws of scalar multiplication hold good for all $\alpha, \beta \in V$, $\alpha, b \in F$.

(1) $a(\alpha+\beta)=a\alpha+a\beta,$

(2) $(a+b)\ \alpha=a\alpha+b\alpha.$

(3) $(ab)\ \alpha=a(b\alpha).$

(4) $1.\alpha=\alpha.$

Here the vector space (to be proved) is $L(V, W)$ whose elements are linear transformations

T_1, T_2 say and let $a, b \in F$

then we have already shown that

$a\ T_1$ is also a L.T. *s.t.* $(a\ T)\ \alpha = a\ [T\ (\alpha)]$

we shall now show that $L(V, W)$ satisfies the above four laws of scalar multiplication.

(i) $[a\ (T_1 + T_2)]\ \alpha = a\ [(T_1 + T_2)\alpha] = a\ [T_1\ (\alpha) + T_2\ (\alpha)]$

$\in W \quad \in W.$

$= a\ T_1\ (\alpha) + a\ T_2\ (\alpha)$ by I for W.

$= (a\ T_1)\ \alpha + (a\ T_2)\ \alpha.$ by def. of $a\ T$.

$= (aT_1 + aT_2)\ \alpha$ by def. of addition of L.T.s.

$\therefore \quad \mathbf{a\ (T_1 + T_2) = aT_1 + aT_2.}$

(ii) $[(a+b)\ T]\ \alpha = (a+b)\ [T\ (\alpha)]$

$\in W$

$= a\ [T\ (\alpha)] + b\ [T\ (\alpha)]$ by 2 for W.

$= (aT)\ \alpha + (bT)\ \alpha.$ by def. of aT.

$= (aT + bT)\ \alpha$ by def. of addition of L.T.s.

$\therefore \quad \mathbf{(a+b)\ T = aT + bT.}$

(iii) $[(ab)\ T]\ \alpha = (ab)\ [T\ (\alpha)] = a\ [b\ T\ (\alpha)]$. by 3 for W

$\in W$

$= a[(b\ T)\ \alpha]$ by def. of aT.

$= [a\ (bT)]\ \alpha.$

$\therefore \quad \mathbf{(ab)\ T = a\ (bT)}$

(iv) $(1.T)\ \alpha = 1\ [T\ (\alpha)] = T\ (\alpha)$. by 4 for W.

$\in W$

$\therefore \quad \mathbf{1.T = T.}$

Thus all the axioms of a vector space are satisfied by $L\ (V, W)$ which therefore is a vector space.

§ 19. Composite Transformation. **(Kanpur 69)**

Let U, V, W be three vector spaces over the same field F.

Let T_1 and T_2 be two linear transformations defined as below

$$T_1 : V \to W, \quad T_2 : U \to V$$

then T_1T_2 is a composite transformation from $U \to W$ defined as

$$T_1T_2(\alpha) = T_1[T_2(\alpha)] \in W.$$
$$\in V$$

Above shows that $T_2 : U \to V$ transforms

$$\alpha \in U \text{ to } T_2(\alpha) \in V$$

and $T_1 : V \to W$ transforms

$$T_2(\alpha) \in V \text{ to } T_1[T_2(\alpha)] \in W.$$

Thus T_1 T_2 is a transformation from U to W.
$V \to W$ $U \to V$

Hence T_1T_2 is defined if the range of post factor T_2 i.e. V is equal to domain of prefactor T_1 i.e. V.

It may be noted that in the composite transformation T_1T_2, T_2 is applied first even though it is written after T_1.

In this case though T_1T_2 is defined but T_2T_1 is not defined because applying $T_1 : V \to W$ it will carry $\beta \in V$. to $T_1(\beta) \in W$. and now $T_2[T_1(\beta)]$ is meaningless as
W.
T_2 is a transformation from $U \to V$. *i.e.* T_2 carries elements of U to V and not elements of W. We can also say that T_2T_1 is not defined because range of postfactor T_1 *i.e.* W is not equal to domain of prefactor T_2 which is U.

To prove that T_1T_2 is linear.

Let $\alpha, \beta \in U$ and $c \in F$ so that $c\alpha+\beta \in U$

Now $T_1T_2[(c\alpha+\beta)] = T_1[T_2(c\alpha+\beta)]$

$= T_1[cT_2(\alpha)+T_2(\beta)]$ as $T_2 : U \to V$ is linear
$\in V$ $\in V$

$= T_1[cT_2(\alpha)]+T_1[T_2(\beta)]$ as $T_1 : V \to W$ is linear

$= cT_1[T_2(\alpha)]+T_1[T_2(\beta)]$

$= c(T_1T_2)\alpha+(T_1T_2)\beta.$

Hence T_1T_2 is a linear transformation.

§ 20. Composite linear operator.

We have seen in last article that if

$T_1 : V \to W$ and $T_2 : U \to V$ then T_1T_2 is a linear transformation from $U \to W$ whereas T_2T_1 is not defined. However in the case of linear operators *i.e.* when $U=V=W$. then both T_1T_2 and T_2T_1 will be defined but T_1T_2 is not in general equal to T_2T_1 *i e.* multiplication of linear operators is not commutative in general. Let us illustrate this by the following examples.

Exercise 6

Ex. 1. *Let T_1 and T_2 be linear operators (L.O.) from R^2 (R) to R^2 (R) defined as follows.*

$$T_1(x_1, x_2)=(x_2, x_1) \quad \ldots(1)$$

$$T_2(x_1, x_2)=(x_1, 0) \quad \ldots(2)$$

Now $T_1T_2(x_1, x_2)=T_1[T_2(x_1, x_2)]$ by def. of T_1T_2

$=T_1[(x_1, 0)]$ by (2)

$=(0, x_1)$ by (1)

Again $T_2T_1(x_1, x_2)=T_2[T_1(x_1, x_2)]$ by def. of T_2T_1

$=T_2(x_2, x_1)$ by (1)

$=(x_2, 0)$ by (2)

Above shows that $T_1T_2 \neq T_2T_1$ *i.e.* T_1 and T_2 are not commutative.

As an other example let us consider the following.

Ex. 2. *Let V be the vector space of all polynomial functions f in one indeterminate x with real coefficients. Let D be the differential operator and let T be the linear operator multiplication by x.*

$$[DT]f(x)=D[Tf(x)]=D[x f(x)]$$

$$=1.f(x)+x f'(x) \quad \ldots(1)$$

$$[TD]f(x)=T[Df(x)]$$

$$=T\left[\frac{df}{dx}\right]=x\frac{df}{dx}=xf'(x) \quad \ldots(2)$$

Hence $DT \neq TD$.

In fact $[(DT-TD)]\, f(x)-f(x)=I\,[f(x)]$

$\therefore \quad DT-TD=I$ *i.e.* the identity operator

Also prove that $(TD)^2=T^2D^2+TD$

$(TD)^2 f(x)=TD\,[(TD)\, f(x)]=TD\,[xf'(x)]$ by (2)

$$=T\{D\,[xf'(x)]$$
$$=T\,[f'(x)+xf''(x)]$$
$$=xf'(x)+x^2 f''(x) \qquad \ldots(3)$$

Again $(T^2D^2)\, f(x)=T^2\,[D^2 f(x)$
$$=T^2\,[f''(x)]=x^2 f''(x)$$

Also $(TD)\, f(x)=xf'(x)$ by 2.

$\therefore \quad (T^2D^2+TD)\, f(x)=x^2 f''(x)+xf'(x)$
$$=(TD)^2 f(x). \text{ by (3)}$$

$\therefore \quad (TD)^2=T^2D^2+TD.$

Ex. 3. *In the vector space of Ex. 2. if the operator T be defined as*

$$T(f(x))=\int_0^x f(x)\,dx.$$

then $DT=I$ *but* $TD \neq I$.

Let $f(x)=p_0+p_1x+p_2x^2+\ldots\ldots \in V$.

$$(DT)\, f(x)=D\,[T\{f(x)\}]=D\left[\int_0^x f(x)\,dx\right]$$
$$=D\left[\int^x\left(p_0+p_1x+p_2x^2+\ldots\ldots\right)dx\right]$$
$$=D\left[p_0x+p_1\frac{x^2}{2}+p_2\,\frac{x^3}{3}+\ldots\right]_0^x$$
$$=\frac{d}{dx}\left[p_0x+p_1\frac{x^2}{2}+p_2\frac{x^3}{3}+\ldots\right]$$
$$=p_0+p_1x+p_2x^2+\ldots=f(x)=I\,[f(x)]$$

Since $(DT)\, f(x)=I\,[f(x)]\ \forall\ f(x) \in V$

$\therefore \quad DT=I$ the identity operator.

$$(TD)\, f(x) = T[D(f(x)]$$
$$= T\left[\frac{d}{dx}(p_0 + p_1x + p_2x^2 + \ldots)\right]$$
$$= T[p_1 + 2p_2x + \ldots]$$
$$= \int_0^x (p_1 + 2p_2x + \ldots)\, dx$$
$$= \left[p_1x + p_2x^3 + \ldots\right]_0^x$$
$$= p_1x + p_2x^2 + \ldots \neq f(x) \neq I[f(x)]$$

$\therefore \quad TD \neq I.$

Hence $DT \neq TD.$

§ 21. Properties of multiplication of linear operators.

Let A, B, C be three linear operators on a vector space V (F) and **O** *and I are the zero and identity operators on V.*

Then the following algebraic results hold good.

(1) $\mathbf{AO} = \mathbf{OA} = \mathbf{O}$

(2) $\mathbf{AI} = \mathbf{IA} = \mathbf{A}$

(3) $\mathbf{A}(\mathbf{B}+\mathbf{C}) = \mathbf{AB}+\mathbf{AC}$. **Right distributive law.**

(4) $(\mathbf{A}+\mathbf{B})\,\mathbf{C} = \mathbf{AC}+\mathbf{BC}$. **Left distributive law.**

(5) $\mathbf{A}(\mathbf{BC}) = (\mathbf{AB})\,\mathbf{C}$. **Multiplication is associative.**

(6) $\mathbf{k}(\mathbf{AB}) = (\mathbf{kA})\,\mathbf{B} = \mathbf{A}(\mathbf{kB})$ **where k is a scalar.**

i.e. multiplication by scalar is associative.

Let $\alpha \in V$ then by definition $I(\alpha) = \alpha$, $\mathbf{O}(\alpha) = \mathbf{0} \in V.$

$AB(\alpha) = A[B(\alpha)].$

(1) $A\,\mathbf{O}(\alpha) = A[\mathbf{O}(\alpha)] = A(0) = \mathbf{0} = \mathbf{O}(\alpha),$

$\therefore \quad A\mathbf{O} = \mathbf{O}$

$\mathbf{O}A(\alpha) = \mathbf{O}[A(\alpha)] = \mathbf{O}(\beta)$ where $\beta = A(\alpha) \in V.$

$= \mathbf{0} = \mathbf{O}(\alpha). \quad \therefore \quad \mathbf{O}A = \mathbf{O}.$

2. $AI(\alpha) = A[I(\alpha)] = A\alpha. \quad \therefore \quad I(\alpha) = \alpha.$

$\therefore \quad AI = I$

$IA(\alpha)=I[A(\alpha)]=I[\beta]$ where $A(\alpha)=\beta$

$=\beta=A(\alpha)$

$\therefore \quad IA=A. \qquad \therefore \quad AI=IA=A.$

3. $[A(B+C)]\alpha=A[(B+C)\alpha]=A[B(\alpha)+C(\alpha)]$

$\in V \quad \in V$

$=A[B(\alpha)]+A[C(\alpha)]$ by linearity of A.

$=(AB)\alpha+(AC)\alpha=(AB+AC)\alpha.$

$\therefore \quad A(B+C)=AB+AC$

4. $[(A+B)C]\alpha=(A+B)[C(\alpha)]$

$\in V$

$=A[C(\alpha)]+B[C(\alpha)]$

by def. of addition.

$=(AC)\alpha+(BC)\alpha$

$=(AC+BC)\alpha.$

$\therefore \quad (A+B)C=AC+C$

$[A(BC)]\alpha=A[(BC)\alpha]=A[B\{C(\alpha)\}]$

$=[\{AB\}C(\alpha)]=[(AB)C]\alpha.$

$\therefore \quad A(BC)=(AB)C.$

5. $[k(AB)]\alpha=kA[B(\alpha)]=[(kA)B(\alpha)].$

$=[(kA)B]\alpha.$

$\therefore \quad k(AB)=(kA)B.$ ...(1)

Again $[A(kB)]\alpha=A[(kB)\alpha]=A[kB(\alpha)]$

$=kA[B(\alpha)]=k[(AB)\alpha]$

$\therefore \quad A(kB)=k(AB)$ ...(2)

$\therefore \quad k(AB)=(kA)B=A(kB)$

Algebra

§ 22. *Define Algebra and prove that the set $L(V, V)$ of all linear operators on V constitutes an algebra.*

Definition. Let $V(F)$ be a vector space over the field F. Then $V(F)$ will be called an algebra over F if it is equipped with another composition called **multiplication** of vectors satisfying the following :

(1) Multiplication is associative

i.e. $$(\alpha\beta)\,\gamma=\alpha\,(\beta\gamma).$$

(2) Multiplication is both right and left distributive

i.e. $$\alpha\,(\beta+\gamma)=\alpha\beta+\alpha\gamma$$
$$(\alpha+\beta)\,\gamma=\alpha\gamma+\beta\gamma.$$

(3) Multiplication by scalar is associative

i.e. $$c\,(\alpha\beta)=(c\alpha)\,\beta=\alpha\,(c\beta).$$

Alternate definition.

Recalling the definition of ring we know that $(R, +, .)$ is a ring if

(a) $(R, +)$ is an abelian group w.r.t. addition.

(b) Multiplication composition is associative.

(c) Multiplication is both right and left distributive w r.t. addition.

The properties (b) and (c) are same as 1 and 2 given in first definition.

Hence we can define algebra as a ring $(R, +, .)$ if the **set R is a vector space with the additional property that**

$$c\,(\alpha\beta)=(c\alpha)\,\beta=\alpha\,(c\beta)$$

i.e. multiplication by scalars is associative which is property 3.

In other words.

A ring $(R,+,.)$ along with an external composition known as scalar multiplication satisfying the laws of scalar multiplication along with the property that

$$c\,(\alpha\beta)=(c\alpha)\quad=\alpha\,(c\beta)$$

is called an algebra.

Algebra with unity.

In case there exists an element in $V\,(F)$ such that

$$1\,.\;\alpha=\alpha.\;1=1$$

then it is said to be an algebra with unity.

Commutative Algebra.

If the elements of V are commutative for multiplication then it is called commutative Algebra.

Thus we see that whereas in a group there is one composition (internal) and in a vector space there are two compositions namely addition of vectors (internal composition) and scalar multiplication of vectors (external composition). But in an algebra there are three compositions, the two being the same as of vector space and the third an internal composition known as "multiplication of vectors" sastifying certain axioms listed above.

2nd part. The set $L(V, V)$ whose elements are linear operators A, B, C is a vector space as has been established in Th. P 24. 377. Again from § 21 P. 283 we know that multiplications of operators satisfies the following

(1) $(AB)\,C=A\,(BC)$

(2) $A\,(B+C)=AB+AC$

$(A+B)\,C=AC+BC$

(3) $k\,(AB)=(kA)\,B=A\,(kB)$.

Also $IA=AI=A$

Hence $L\,(V, V)$ is an algebra with unity.

Similarly the set of $n\times n$ matrices with elements over R is an algebra over R with identity.

Another Theorem. The set $L(V, V)$ of all linear operators on a vector space V is a ring with unity element with respect to addition and multiplication of operators defined as before.

§ 23. LINEAR FUNCTIONAL ON VECTOR SPACE (V. S.)

Linear Functionals.

If $V(F)$ and W $(F$ vector spaces over the same field F then

1. $T: V \to W$ is a linear transformation from V to W.
2. $T: V \to V$ is a linear operator from V to V.
3. $f: V \to F$ *i.e.* f is a linear trasformation from a vector space V to its field F then this particular type of transformation is said to be linear functional (L.F.).

Hence a linear functional f over $V(F)$ is a mapping which assigns to each member $\alpha \in V(F)$ an element $f(\alpha)$ which is in F, such that f is linear.

In other words

$$f(\alpha+\beta)=f(\alpha)+f(\beta) \qquad \alpha, \beta \in V$$
$$f(a\,\alpha)=a\,f(\alpha) \qquad a \in F$$

Combinning the above two we can define linearity by a single relation *i.e.* $f(a\,\alpha+\beta)=a\,f(\alpha)+f(\beta)$.

Zero functional : If $f(\alpha)=0$ (scalar) $\forall\ \alpha \in V(F)$ then f is said to be zero functional and is denoted by **O**. Similarly $(-f)\,\alpha=-f(\alpha)$ and we can show that both **O** and $-f$ are alsol inearfu nctionals as shown on P. 375–376 that **O** and $-T$ are also linear transformations.

Exercise 6

Ex. 1. *Let us consider the vector space $R^n(R)$.*

Let $\alpha \in R^n(R)=(a_1, a_2, \ldots, a_n)$ $a_i \in R$ *i.e.* F
$\beta \in R^n(R)=(b_1, b_2, \ldots, b_n)$, $b_i \in R$ *i.e.* F.

Let us define a mapping f which sends each $\alpha \in R^n(R)$ to its first coordinate *i.e.* $a_1 \in R$ *i.e.* F.

$$f: \alpha \to a_1 \quad i\,e. \quad f(\alpha)=a_1$$
$$f: \beta \to b_1 \quad i.e. \quad f(\beta)=b_1.$$

The above mapping is a functional as it sends the elements of the vector space to its field and we have only to establish its linearity. Consider any element $c\alpha+\beta \in R^n(R)$

$$c\alpha+\beta=c\,(a_1, a_2, \ldots, a_n)+(b_1, b_2,\ldots,b_n)$$
$$=c\,a_1+b_1, c\,a_2+b_2,\ldots,c\,a_n+b_n. \qquad \ldots(A)$$

$\therefore$ $f(c\alpha+\beta)=ca_1+b_1$ by definition of f *i.e.* it sends each element of vector space $R^n(R)$ to its first coordinate in R.

or $$f(c\,\alpha+\beta)=c\,f(\alpha)+f(\beta). \quad \text{by (A)}$$

Hence f is linear.

Ex. 2. *In example 1 if $x_1, x_2, x_3, \ldots, x_n$ be fixed elements of R i.e. F then a functional f defined as under*

$$f(\alpha)=x_1\,a_1+x_2\,a_2+\ldots\ldots+x_n\,a_n$$

is a linear functional.

If $\beta=(b_1, b_2,\ldots,b_n)$ then

$f(\beta)=x_1\,b_1+x_2\,b_2+\ldots\ldots+x_n\,b_n$.

Now $c\,\alpha+\beta=(c\,a_1+b_1, c\,a_2+b_2,\ldots\ldots,ca_n+b_n)$.

$\therefore f(c\,\alpha+\beta)=x_1\,(c\,a_1+b_1)+x_2\,(ca_2+b_2)+\ldots\ldots$
$$+x_n\,(ca_n+b_n)$$
by definition of f
$$=c\,(x_1\,a_1+x_2\,a_2+\ldots+x_n\,a_n)$$
$$+(x_1\,b_1+x_2\,b_2+\ldots+x_n\,b_n)$$
$$=c\,f(\alpha)+f(\beta).$$

Hence f is linear. Also

$$x_i \in F, a_i \in F \Rightarrow \Sigma\, x_i\, a_i \in F.$$

$\therefore$ $f(\alpha)=\Sigma\, x_i\, a \Rightarrow f: R^n(R) \to R$ *i e.* F.

Hence f is a linear functional.

Ex. 3. *Let V be the set of all $n \times n$ matrices over a field F (i e, R) Let $A=[a_i]$ where $a_{ij} \in F$ then we know that*

Trace A = sum of the diagonal elements of A

$$= a_{11} + a_{22} + \ldots + a_{nn} \in F.$$

Now if f be a mapping which sends each matrix A of the vector space V to trace A which is in F

$f : A \to$ Trace A. or $f(A) =$ Trace A. then f will be a linear functional if we establish the linearity of f

Let A, B be any two square matrices $\in V$

The matrix $cA + B$ will have its diagonal elements

$ca_{11} + b_{11}$, $ca_{22} + b_{22}, \ldots, ca_{nn} + b_{nn}$

$f(cA + B) =$ Trace $(cA + B)$

$= ca_{11} + b_{11} + ca_{22} + b_{22} + \ldots + ca_{nn} + b_{nn})$

$= c(a_{11} + b_{22} + \ldots + a_{nn}) + (b_{11} + b_{22} + \ldots + b_{nn})$

$= c$ Trace $A +$ Trace B

$f(cA + B) = cf(A) + f(B)$ so that f is linear functional.

Theorem 25. *If f be a linear functional on a vector space V (F) then*

(a) $f(0) = 0$

(b) $f(-\alpha) = -f(\alpha)\ \forall\ \alpha \in V$.

Since f is a linear functional hence $\alpha \in V \Rightarrow f(\alpha) \in F$

$\therefore$ $f(\alpha) + 0 = f(\alpha)$ where 0 is zero of F

or $f(\alpha) + 0 = f(\alpha + 0)$ $\because$ $\alpha + 0 = \alpha$.

$\Rightarrow f(\alpha) + 0 = f(\alpha) + f(0)$ $\therefore$ f is linear

$\Rightarrow f(0) = 0$ by cancellation law in F

(ii) $f[\alpha + (-\alpha)] = f(\alpha) + f(-\alpha)$ as f is linear

or $f(0) = f(\alpha) + f(-\alpha)$ $\because$ $\alpha + (-\alpha) = 0$

or $0 = f(\alpha) + f(-\alpha)$

Above relation shows that $f(-\alpha)$ is the additive inverse of $f(\alpha)$ in F which is $f(\alpha)$

or $f(-\alpha) = -f(\alpha)$

§ 24 Dual space of vector space V (F).

We have already proved that the set $L(V, W)$ of all linear transformations $T : V \to W$ is a vector space w.r.t. the two compositions namely addition of transformations and scalar multiplication of a linear transformation defined as under

$$(T_1+T_2)\,\alpha = T_1\alpha + T_2\alpha.$$

$$(aT)\,\alpha = a\,[T(\alpha)]$$ (see Th. 24 P. 377)

Similarly the set of all linear functionals f on V denoted by $L(V, F)$ (F is regarded both as a field and a vector space $F(F)$, is a vector space w.r.t. the two compositions defied as above.

i.e. $(f_1+f_2)\,\alpha = f_1(\alpha)+f_2(\alpha) \;\forall\; \alpha \in V$

$(af)\,\alpha = a\,[f(\alpha)] \;\forall\; \alpha \in V,\ a \in F.$

This vector space of all linear functionals on V

i e. $L(V, F)$ *is called the dual space of V and is denoted by V^**

Hence $V^* = \{f : V \to F$ such that f is linear.$\}$

Theorem 26. *The set V^* of all linear functionals on a vector space $V(F)$ is also a vector space over the field F with addition and scalar multiplication defined as*

$$(f_1+f_2)\,\alpha = f_1(\alpha)+f_2(\alpha) \;\forall\; \alpha \in V \quad \ldots(1)$$

$$(af)\,\alpha = a\,[f(\alpha)] \;\forall\; \alpha \in V,\ a \in F \quad \ldots(2)$$

First of all we shall prove that f_1+f_2 and af are linear functionals which in other words means that the set V^* is closed both for addition and scalar multiplication.

Since $f_1(\alpha), f_2(\alpha) \in F$ it follows from I that

$(f_1+f_2)\,\alpha \in F$ *i e.* $f_1+f_2 : V \to F$

and as such f_1+f_2 is a functional.

Similarly $f(\alpha) \in F, a \in F \Rightarrow a\,[f(\alpha)] \in F$ and hence from (2) we get $(af)\,\alpha \in F$

i.e. $af : V \to F$ so that (af) is also a functional.

Linearity of f_1+f_2

Let $\alpha, \beta \in V$ and $c \in F$

$(f_1+f_2)(c\alpha+\beta)=f_1(c\alpha+\beta)+f_2(c\alpha+\beta)$ by I

$=cf_1(\alpha)+f_1(\beta)+cf_2(\alpha)+f_2(\beta)$

by linearity of f_1, f_2.

$=c[f_1(\alpha)+f_2(\alpha)]+f_1(\beta)+f_2(\beta)$

$=c[(f_1+f_2)\alpha]+(f_1+f_2)\beta$ by I

Hence f_1+f_2 is also linear

Thus $f_1, f_2 \in V^* \Rightarrow f_1+f_2 \in V^*$.

Linearity of a f.

$(af)(c\alpha+\beta)=a[f(c\alpha+\beta)]$ by (2)

$=a[cf(\alpha)+f(\beta)]$ $\because$ f is linear

$=a[cf(\alpha)]+a[f(\beta)]$ by Dist. Law in a field

$=(ac)f(\alpha)+a[f(\beta)]$

$=(ca)f(\alpha)+a[f(\beta)]$

$\because$ $ac=ca$ in a field.

$=c[af(\alpha)]+a[f(\beta)]$

$=c[(af)\alpha]+(af)\beta$

Hence af is also linear

Thus $f \in V^*, a \in F \Rightarrow af \in V^*$

Hence the set V^* of all linear functionals is closed both for addition and scalar multiplication.

Axioms of vector space.

The set $(V^*, +)$ is an abelian group.

1. Closure property. $f_1, f_2 \in V^* \Rightarrow f_1+f_2 \in V^*$

This we have already proved above.

2. Associative. $(f_1+f_2)+f_3=f_1+(f_2+f_3)$

$[(f_1+f_2)+f_3]\alpha=(f_1+f_2)\alpha+f_3(\alpha)\ \forall\ \alpha \in V$ by I

$=[f_1(\alpha)+f_2(\alpha)]+f_3(\alpha)$ by I

$=f_1(\alpha)+[f_2(\alpha)+f_3(\alpha)]$

As $f_1(\alpha), f_2(\alpha), f_3(\alpha)$

all belong to F in which addition is associative.

$$=f_1(\alpha)+(f_2+f_3)\alpha. \text{ by } I$$
$$=[f_1+(f_2+f_3)]\alpha. \ \forall\ \alpha \in V$$

$\therefore\ (f_1+f_2)+f_3=f_1+(f_2+f_3)$.

3. Identity. The zero functional $\mathbf{O}$ *s.t.* $\mathbf{O}(\alpha)=0 \in F$ is the identity of V^*

$\therefore\ (f+\mathbf{O})\ \alpha=f(\alpha)+\mathbf{O}(\alpha)\ \forall\ \alpha \in V$
$$=f(\alpha)+0=f(\alpha).$$

as 0 is the identity of F.

$\therefore\ f+\mathbf{O}=f$. similarly $\mathbf{O}+f=f$.

4. Inverse. The inverse of any functional $f \in V^*$ is $-f \in V^*$ such that

$$(-f)\ \alpha=-[f(\alpha)] \text{ by definition.}$$
$$[f+(-f)]\alpha=f(\alpha)+(-f)\ \alpha \text{ by } I$$
$$=f(\alpha)-f(\alpha) \text{ by def of } -f.$$
$$=0 \in F=\mathbf{O}(\alpha)\ \forall\ \alpha \in V$$
by def. of $\mathbf{O}$ functional.

$\therefore\ f+(-f)=\mathbf{O}$. Similarly $(-f)+f=\mathbf{O}$

5. Commutative. *i.e.* $f_1+f_2=f_2+f_1\ \forall\ f_1, f_2 \in V^*$

$(f_1+f_2)\ \alpha=f_1(\alpha)+f_2(\alpha)$ by I
$$=f_2(\alpha)+f_1(\alpha)$$

$\because$ Addition in F is commutative.
$$=(f_2+f_1)\ \alpha\ \forall\ \alpha \in V \text{ by } I$$

$\therefore\ f_1+f_2=f_2+f_1$

Hence $(V^*, +)$ is an additive abelian group.

B. Laws of scalar multiplication.

For any vector space V the following laws of scalar multiplication hold good.

$\alpha, \beta \in V$, $a, b \in F$. we have

(1) $a(\alpha+\beta)=a\alpha+a\beta$.
(2) $(a+b)\ \alpha=a\alpha+b\alpha$
(3) $(ab)\ \alpha=a[b(\alpha)]$
(4) $1\cdot\alpha=\alpha$.

Here the elements of set V^* are linear functional f_1, f_2 say and let $a, b \in F$ then we have alrady proved that af_1 is also a linear functional such that

$$(af_1)\ \alpha = a\,[f_1(\alpha)].$$

We will now show that the elements of V^* satisfy the above four laws.

(1) $[a(f_1+f_2)]\,\alpha = a\,[(f_1+f_2)\,\alpha] = a\,[f_1(\alpha)+f_2(\alpha)]$
$= af_1(\alpha)+af_2(\alpha)$ by Dist-Law in F
$= (af_1)\,\alpha+(af_2)\,\alpha$ by def. of af
$= (af_1+af_2)\,\alpha$. by def. of addition in V^*
$\therefore\quad a(f_1+f_2) = af_1+af_2.$

(2) $[(a+b)f]\,\alpha = (a+b)\,[f(\alpha)]$ by def. of af.
$= af(\alpha)+bf(\alpha)$ by Dist-Law in F
$= (af)\,\alpha+(bf)\,\alpha$ by def. of af
$= (af+bf)\,\alpha$. by def. of addition in V^*
$\therefore\quad (a+b)f = af+bf.$

(3) $[(ab)f]\,\alpha = (ab)\,[f(\alpha)]$ by def. of af
$= a\,[b\,f(\alpha)]$
$\because$ Multiplication in F is associative.
$= a\,[(bf)\,\alpha]$ by def. of bf.
$= [a\,(bf)]\,\alpha.$
$\therefore\quad (ab)f = a\,(bf)$

(4) $(1.f)\,\alpha = 1\,[f(\alpha)]$ by def. of af
$= f(\alpha)$
as 1 is the multiplicative identity of field.
$\therefore\quad 1.f = f.$

Hence V^* the set of all linear functionals on V is a vector space w.r.t. addition and scalar multiplication as defined in 1 and 2.

The vcetor space V^* is called the **dual space of vector space** V.

Theorem 27. *If $V(F)$ is an n dimensional vector space and set*

$A=\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *be an ordered basis for V then for any set of n scalars.*

$B=\{x_1, x_2, \ldots, x_n\}$ *there exists a unique linear functional f on V such that*

$$f(\alpha_i)=x_i,\ i=1, 2, \ldots, n.$$

Refer Theorem 22. P. 369.

Proof. Let $\alpha \in V \Rightarrow \alpha=a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n$ as A is a basis. For this vector α let us define f as under

$$f(\alpha)=a_1x_1+a_2x_2+\ldots+a_nx_n \qquad \ldots(1)$$

i.e. we have chosen the same scalars $a_1, a_2, \ldots, a_n$ which were used for expressing α.

Since $a_i' \in F, x_i' \in F \quad \therefore \quad \Sigma a_i x_i \in F.$

Thus from *1* we conclude that f is a mapping which associates each $\alpha \in V$ to an element of F. Thus $f: V \to F$.

f is linear.

Let $\beta \in V \quad \therefore \quad \beta=b_1\alpha_1+b_2\alpha_2+\ldots+b_n\alpha_n.$

For this vector β let us define

$$f(\beta)=b_1x_1+b_2x_2+\ldots+b_nx_n. \qquad \ldots(2)$$

Now $c\alpha+\beta=c(a_1\alpha_1+a_2\alpha_2+\ldots+a_n\alpha_n)$
$$+(b_1\alpha_1+b_2\alpha_2+\ldots+b_n\alpha_n)$$
$$=(ca_1+b_1)\alpha_1+\ldots+(ca_n+b_n)\alpha_n$$
$$\therefore \quad f(c\alpha+\beta)=(ca_1+b_1)x_1+\ldots+(ca_n+b_n)x_n.$$

We have chosen the same scalars which we used in representation of $c\alpha+\beta$ in terms of basis set.

$$\therefore \quad f(c\alpha+\beta)=c(a_1x_1+a_2x_2+\ldots+a_nx_n)$$
$$+(b_1x_1+b_2x_2+\ldots+b_nx_n)$$
$$=cf(\alpha)+f(\beta) \quad \text{by 1 and 2}$$

Hence f is linear.

Again from above definition of f we have

$$\alpha_i = 0\alpha_1 + 0\alpha_2 + \ldots + 1.\alpha_i + \ldots + 0\alpha_n$$

$\therefore \quad f(\alpha_i) = 0x_1 + 0x_2 + \ldots + 1.x_i + \ldots + 0.x_n$ by I

or $\quad f(\alpha_i) = x_i \quad \because \quad 1.x_i = x_i$ in a field F.

Hence $f(\alpha_i) = x_i$, $i = 1, 2, \ldots, n$.

Uniqueness of f. Let g be any other linear functional such that $\quad g(\alpha_i) = x_i \ \forall \ i$.

Now $g(\alpha) = g(a_1\alpha_1 + a_2\alpha_2 + \ldots + a_n\alpha_n)$

$= a_1 g(\alpha_1) + a_2 g(\alpha_2) + \ldots + a_n g(\alpha_n)$

by linearity of g

$= a_1x_1 + a_2x_2 + \ldots + a_nx_n \quad \because \quad g(\alpha_i) = x_i$

$= f(\alpha)$ by (1)

Since $g(\alpha) = f(\alpha) \ \forall \ x \in V \quad \therefore \quad g = f$.

Hence above establishes the uniqueness of f.

§ 25. Dimensions of the dual space.

Theorem 28. *The number of elements in the basis set of V^* the dual space of V is called the dimension of dual space.*

The dual space V^* of a finite dimensional vector space $V(F)$ of dim n is itself of dimension n.

Or

If $V(F)$ is an n dimensional vector space and

$$S_1 = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$$

is a basis for V then there exists a unique basis

$$S_2 = \{f_1, f_2, \ldots, f_n\}$$

of the dual space V^* with the property that

$$f_j(\alpha_i) = \delta_{ij}, \ j = 1, \ldots, n$$

where δ_{ij} is the Kronecker Delta which means that

$f_j(\alpha_i) = 0 \quad i \neq j$

$f_i(\alpha_i) = 1 \quad i = j$ **(Meerut 69)**

Given. The vector space $V(F)$ is finite dimensional and has dimension n and hence it has a basis set S_1 consisting of n vectors *i.e.*

$S_1=\{\alpha_1, \alpha_2, .., \alpha_n\}$ is a basis for V. ...(1)

so that any vector $\alpha \in V$ can be uniquely expressed as

$$\alpha=\sum_{i=1}^{n} a_i\alpha_i \qquad \ldots(2)$$

To prove dim V*=n. In order to prove that dimension of dual space V^* is also n we have to establish that there exists a basis consisting of n elements of V^* which are linear functionals.

$S_2=\{ f_1, f_2 ,..., f_n\}$ where $f_i's$ are in V^* and are linear functionals on V is a basis set for V^*.

Method.

In order to prove this we will have to establish the following.

(1) S_2 is linearly independent.

(2) S_2 is a spanning set for V^* *i.e.* any functional $f \in V^*$ is expressible as a l.c. of $f_i's$ the elements of basis set S_2.

Proof.

Step. 1. Let us define the linear functional f_j on V as follows

$\alpha \in V=a_1\alpha_1+a_2\alpha_2+...+a_n\alpha_n$ and let

$f_j(\alpha)=f_j(\Sigma a_i\alpha_i)=a_j \in F$ (By definition)

In other words f_j assigns to each vector α in V the jth coordinate of α, relative to its basis S_1.

Clearly f_j is a functional and we must establish its linearity,

Let $\alpha, \beta \in V$ and $c \in F$ so that $\alpha=\Sigma a_i\alpha_i$, $\beta=\Sigma b_i\alpha_i$

$\therefore \quad c\alpha+\beta=c\ \Sigma\ a_i\alpha_i+\Sigma b_i\alpha_i=\Sigma\ (ca_i+b_i)\ \alpha_i$

$\therefore \quad f_j(c\alpha+\beta)=ca_j+b_j$ (by definition)

$=c\ f_j(\alpha)+f_j(\beta).$

Hence f_j is linear.

Also $f_j(\alpha_i)=f_j(0\alpha_1+0\alpha_2+\ldots+1.\alpha_i+\ldots+0\alpha_n)=0$

i.e. as $a_j=0$

$f_j(\alpha_j)=f_j(0\alpha_1+0\alpha_2+\ldots+1.\alpha_j+\ldots+0\alpha_n)=1$ as $a_j=1$

or $f_j(\alpha_i)=\delta_{ij}$ which means $=0$, $i\neq j$, $=1$, $i=j$.

Uniqueness of f. If g_j be any other functional s.t.

$$g_j(\alpha_i)=\delta_{ij} \text{ then}$$

$g_j(\alpha)=g_j(\sum_i a_i\alpha_i)=\sum_i a_i g_j(\alpha_i)$ by Linearity of g_j

$$=a_j=f_j(\alpha) \quad \therefore \quad g_j=f_j.$$

Hence f_j is unique.

Step 2. The set S_2 is linearly independent.

Consider a linear relation $\Sigma c_i f_i = O$ *i.e.* zero functional say f and we shall show that each $c_i=0$ in order to establish the L I of S_2.

Now $f(\alpha_j)=O(\alpha_j)=0$ for each j as f is a zero functional

Put $f=\Sigma c_i f_i$ in the L.H.S.

$$\therefore \quad \Sigma (c_i f_i)\alpha_j=0 \Rightarrow \Sigma c_i (f_i \alpha_j)=0$$

$$\Rightarrow \sum_{i=1}^{n} c_i \delta_{ij}=0 \Rightarrow c_j.1=0$$

because $i\neq j$, $\delta_{ij}=0$ and when $i=j$ then $\delta_{ij}=1$.

Now in place of α_j we could take any of the $\alpha_1, \alpha_2, \ldots, \alpha_n$ and thus prove that

$$c_1=0,\ c_2=0,\ \ldots,c_n=0.$$

Thus $c_i=0$ for each i and hence the set S_2 is L.I.

Step 3. To prove that S_2 spans V^*

Let f be any functional $\in V^*$ such that $f(\alpha_j)=c_j$

Now if $\alpha \in V$ then $\alpha=\Sigma a_i \alpha_i$

$$\therefore \quad f(\alpha)=f(\Sigma a_i \alpha_i)=\Sigma a_i f(\alpha_i)=\Sigma a_i c_i \qquad \ldots(1)$$

Again $(\Sigma c_j f_j)\alpha=(\sum_j c_j f_j)(\sum_i a_i \alpha_i)$

$$=\sum_i c_j f_j (\Sigma a_i \alpha_i)$$

$$=\sum_j c_j \sum_i a_i f_j (\alpha_i) \text{ Linearity of } f_j$$

$$=\sum_j c_j a_j \quad \therefore \quad f_j (\alpha_i)=\delta_{ij}=1 \text{ when } i=j$$
$$=0 \text{ when } i\neq j$$

$$=\sum_i c_i a_i=f (\alpha) \text{ by I.}$$

Thus we have proved that

$$(\Sigma c_j f_j)\ \alpha=f (\alpha) \quad \forall \ \alpha \in V,$$

$\therefore \quad f=\Sigma c_j f_j$ or $[f=\Sigma f (\alpha_j) f_j$ on putting $c_j=f (\alpha_j)]$

i.e. f has been expressed as a L.C. of $f_1, f_2, \ldots, f_n$ and these n functionals have been shown to be L.I. and as such they form a basis for V^*. Since it consists of n elements and as such dim $V^*=n$.

$$\therefore \quad \dim V=\dim V^*=n,$$

Also the set S_2 is unique as each member f_j in it is unique as shown earlier.

This set S_2 is called dual Basis of V^* corresponding to given basis S_1 of V (F).

Cor. *Prove that the vector space V and its dual V^* are isomorphic to each other.*

We know that two vector spaces are isomorphic to each other $\Leftrightarrow$ they have the same dimensions (Th. 23. P. 370)

Here dim $V=\dim V^*=n$.

Hence $V\cong V^*$.

Therefore the proof of the above corollary is same as the proof of the main theorem.

Another form of the above Theorem.

Theorem 29. *If V be a finite dimensional vector space over rhe field F and let*

$$B=\{\alpha_1, \alpha_2,\ldots,\alpha_n\}$$

be a basis for V. Then there is a unique basis

$$B^*=\{f_1, f_2,\ldots, f_n\}$$

for V^* such that

(1) $f_i(\alpha_j)=\delta_{ij}$

(2) $f=\sum_{i=1}^{n} f(\alpha_i) f_i$ *for each l.f. on V.*

(3) $\alpha=\sum_{i=1}^{n} f_i(\alpha)\,\alpha_i$ *for each α in V.*

(1) We have already proved that B^* is a basis for V^* such that

$$f_i(\alpha_j)=\delta_{ij}.$$

(2) We have to show that

$$f=\sum_{i=1}^{n} f(\alpha_i) f_i.$$

Since B^* is a basis for V^*.

$\therefore$ $f \in V^*$ is expressible as a l.c. of f_i's in B^*

$\therefore$ $f=\sum_{i=1}^{n} c_i f_i$ we have to show that $c_i=f(\alpha_i)$.

But $f(\alpha_j)=\sum_{i=1}^{n}(c_i f_i)\,\alpha_j=\sum_{i=1}^{n} c_i\,[f_i(\alpha_j)]$

$=\sum_{i=1}^{n} c_i\,\delta_{ij}=c_j$. On summing w.r.t. i

$\therefore$ $f(\alpha_j)=c_j$ or $f(\alpha_i)=c_i$

$\therefore$ $f=\sum_{i=1}^{n} f(\alpha_i) f_i$

(3) We have to show that $\alpha=\sum_{i=1}^{n} f_i(\alpha)\ \alpha_i$

B is a basis set for V and $\alpha \in V$

$\therefore \quad \alpha=\sum_{i=1}^{n} c_i\ \alpha_i$. We have to show that $c_i=f_i(\alpha)$

Now $f_j(\alpha)=f_j\left(\sum_{i=1}^{n} c_i\ \alpha_i\right)=\sum_{i=1}^{n} c_i\ f_j(\alpha_i)$

$$\sum_{i=1}^{n} c_i\ \delta_{ij}=c_j \quad \therefore \quad f_j(\alpha)=c_i$$

$$\therefore \quad f_i(\alpha)=c_i$$

Hence $\alpha=\sum_{i=1}^{n} c_i\ \alpha_i=\sum_{i=1}^{n} f_i(\alpha)\ \alpha_i$

Theorem 30. *For every non zero vector α in a finite dimensional vector space V there is a linear functional f in V^* such that $f(\alpha)\neq 0$.*

We know that $f_j(\alpha)=f_j(\Sigma\ a_i\ \alpha_i)=\sum_i a_i f_j(\alpha_i)$

$$=\sum_i a_i\ \delta_{ij}=a_j \qquad \ldots(1)$$

Now if $f(x)=0\ \forall\ f \in V^*$ then as a particular case we have $f_1(x)=0, f_2(x)=0,\ldots,f_n(x)=0$ where $\{f_1, f_2,\ldots, f_n\}$ is a basis for V^*

i.e. $$f_j(\alpha)=0 \quad \forall\ j$$

$$\Rightarrow\ a_j=0\ \ \forall\ j \Rightarrow\ \alpha=\Sigma\ a_i\ \alpha_i=0$$

which is a contradiction as α is a non zero vector in V.

Therefore if $\alpha \neq 0$ then for at least one $f \in V^*$ we have $f(\alpha) \neq 0$

Cor. *If* $\alpha \neq \beta$ *then* $\exists$ *a linear functional* f *on* V *such that* $f(\alpha) \neq f(\beta)$.

Since $\alpha \neq \beta \Rightarrow \alpha - \beta \neq 0 \Rightarrow \exists$ a linear functional f on V such that $f(\alpha - \beta) \neq 0$

$\Rightarrow f(\alpha) - f(\beta) \neq 0 \Rightarrow f(\alpha) \neq f(\beta)$.

List of Important question & articles

§ 2 P. 285, Ex. I. P. (286–295) Q. [2, 4, 7,] § 3 P. 296, § 4 P. 298, Th. 3, 4 P. 300.

Th. 6. P. 306, § 10 P. 319, Ex. 4 P. 326, Th. 9. P. 328, Th. 10. P. 337, Th. 11. P. 33 ,

Th. 12. P. 340. Cor. 1, 2, P. 343, Th. 13 P. 344, Th. 14 P. 345, Th. 16 P. 347, Th 17 P. 349.

Th. 18. P. 353, Th. 19. P. 355, Th. 20. P. 363, Th. 21. P. 364, Th. 23. P. 370.

Th. 24. P. 377, § 19, P. 379. § 22 P. 384, Th. 26. P. 389, Th. 28. P. 394.

CHAPTER V

NORMAL SUB GROUPS

§ 1. Introduction. Let G be a group in which the composition is denoted multiplicatively and H be a sub group of G then as defined in § 8 P. 148. $Ha=\{ha : h \in H$ is a right coset of H in G generated by $a \in G$. *i e.* Ha is the set of all those elements of G which are obtained by multiplying the elements of sub group H by $a \in G$ on the right.

Similarly $aH=\{ah : h \in H\}$ is a left coset of H in G generated by $a \in G$ *i e* aH is the set of all those elements of G which are obtained by multiplying the elements of sub group H by a on the left.

In case **G be an abelian** group then we know that

$$ha=ah \quad \forall \ h \in H.$$

and hence we must have $Ha=aH$.

i.e. right and left cosets generated by a coincide.

Since a is arbitrary it follows that

$$Ha=aH \quad \forall \ a \in G.$$

But if **G be not abelian** then also it is possible to have sub groups H of G for which $Ha=aH \ \forall \ a \in G$.

i.e. right and left cosets coincide.

Such sub groups H of G will be called **normal sub groups of G**.

§ 2. Normal sub group.

Definition I. *A sub group H of a group G will be a normal sub group of G if and only if $x \in G$ and $h \in H$ we have $xhx^{-1} \in H$.* (Raj. 66, 67)

Another Definition.

From the definition of normal sub group as given above

i.e. $xhx^{-1} \in H \ \forall \ x \in G$ and $h \in H$ we conclude

that $h \in H \Rightarrow x\,h\,x^{-1} \in H \;\forall\; x \in G$ ...(1)

Since above holds for all $h \in H$ we can say now

$$x\,Hx^{-1}=\{xhx^{-1} : h \in H\}$$

Now if α be any element of xHx^{-1} then

$\alpha=xhx^{-1}$, $h \in H \Rightarrow \alpha \in H$ by I.

Hence $xHx^{-1} \subset H$.

A sub group H of a group G is a normal sub group of G if and only if $x\,Hx^{-1} \subset H$.

From the above definition of normal sub groups, we shall deduce here in below other definitions or criteria for a sub group H to be a normal sub group of G.

§ 3. **Different characterisation of normal sub groups.**

Theorem 1. *A sub group H of a group G is a normal sub group if and only if*

$$xHx^{-1}=H \;\forall\; x \in G.$$

Given $xHx^{-1}=H$. **To prove** H is normal sub group.

Since $xHx^{-1}=H$ hence $xHx^{-1} \subset H$ and hence by definition of normal sub group in § 2 it follows that H is a normal sub group.

Converse. Given H is a normal sub group

i.e. $xHx^{-1} \subset H \;\forall\; x \in G$ ...(1)

To prove that $xHx^{-1}=H$ (2)

The only thing that we have to prove now is that $H \subset xHx^{-1}$ so that the condition along with condition (1) would prove the relation (2)

Now from (1, $xHx^{-1} \subset H \;\forall\; x \in G$. But if $x \in G$ then x^{-1} also $\in G$ which is a group.

Hence replacing x by x^{-1} in 1 we have

$$x^{-1}H\,(x^{-1})^{-1} \subset H \;\forall\; x \in G.$$

$\Leftarrow x^{-1}Hx \subset H, \forall\; x \in G$ as $(x^{-1})^{-1}=x$

$\Rightarrow x\,(x^{-1}\,Hx)\,x^{-1} \subset x\,Hx^{-1}$

$\Rightarrow H \subset xHx^{-1}$.

$\because \quad x\,x^{-1}=e$, and $eH=He=H$

Also $xHx^{-1} \subset H$. by (1)

$\therefore \quad xHx^{-1}=H. \ \forall \ x \in G.$

Note. The relation $xHx^{-1}=H$ implies that if $h \in H$ *i.e.* if $xhx^{-1} \in xHx^{-1}$ then xhx^{-1} will only be an element of H but not equal to h

i.e. $xhx^{-1} \neq h \ \forall \ x \in G$ and $\forall \ h \in H.$

The above will be clear from the following example

From Ex. 3. P. 75, we know that the set of all permutations on three symbols a, b, c is a finite abelian group w.r.t. permutation multiplication as the composition.

$G=\{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6\}$ the composition table being

o	α_1	α_2	α_3	α_4	α_5	α_6
α_1	α_1	α_2	α_3	α_4	α_5	α_6
α_2	α_2	α_1	α_4	α_3	α_6	α_5
α_3	α_3	α_5	α_1	α_6	α_2	α_4
α_4	α_4	α_6	α_2	α_5	α_1	α_3
α_5	α_5	α_3	α_6	α_1	α_4	α_2
α_6	α_6	α_4	α_5	α_2	α_3	α_1

Consider the sub group.

$$H=\{\alpha_1, \alpha_4, \alpha_5\}.$$

H is a normal sub group.

H will be a normal sub group if

$$xHx^{-1}=H \ \forall \ x \in G$$

Choose $\alpha_2 \in G$ then $\alpha_2^{-1}=\alpha_2$ from the table. Also $\alpha_2 \ H \ \alpha_2^{-1}=\{\alpha_2 \ h \ \alpha_2^{-1} : h \in H\}$

$=\{\alpha_2\alpha_1\alpha_2^{-1}, \alpha_2\alpha_4\alpha_2^{-1}, \alpha_2\alpha_5\alpha_2^{-1}\}$.

$\because$ $h \in H$ is $\alpha_1, \alpha_4, \alpha_5\}$.

$=\{(\alpha_2\ \alpha_1)\ \alpha_2, (\alpha_2\ \alpha_4)\ \alpha_2, (\alpha_2\ \alpha_5)\ \alpha_2\}$

$=\{\sigma_2\ \alpha_2, \alpha_3\ \alpha_2, \alpha_6\ \alpha_2\}$ from the table

$=\{\alpha_1, \sigma_5, \alpha_4\}=H$

$\therefore$ $xHx^{-1}=H \quad \forall\ x \in G$ and hence H is a normal sub group.

But $xhx^{-1} \neq h\ \forall\ x \in$ and $\forall\ h \in H$.

because $\alpha_2\alpha_4\alpha_2^{-1}$ is an element of the type xhx^{-1} and it is not equal to α_4,

$\because$ $\alpha_2\sigma_4\alpha_2^{-1}=\alpha_2\alpha_4\alpha_2=(\alpha_2\ \alpha_4)\ \alpha_2=\alpha_3\ \alpha_3=\alpha_5$ *i.e.*$\neq\alpha_4$.

Theorem 2. *A subgroup H of a group G is a normal sub group of G if and only if each right coset of H in G is the left coset of H in G i.e. $xH=Hx \forall x \in G$.* **(Meerut M.Sc. 1969)**

Given H is normal sub group

i e. $xHx^{-1}=H\ \forall\ x \in G$ Theorem. (1).

To prove. Each right coset of H in G is a left coset.

$xHx^{-1}=H \Rightarrow (xHx^{-1})\ x=Hx \Rightarrow xH=Hx\ \forall\ x \in G$.

Hence each right coset of H in G is a left coset.

Converse. Given. Each right coset of H in G is a left coset.

i.e. if $x \in G$ then the right coset Hx is also a left coset xH.

To prove H is a normal sub group

i.e. $xHx^{-1}=H\ \forall\ x \in G$ Th. (1).

Now if $x \in G$ then the right coset $Hx=\{hx : h \in H\}$

but $e \in H$ and $ex=x$ and hence x belongs to right coset Hx.

Now we have to search a left coset say P to which the righs coset Hx is identical.

Since $x \in Hx$ hence the required left coset P must also contain x. But as argued above x also belongs to left coset xH. Thus the two left cosets P and xH have a common

element x and we know that the two cosets (right and left) are either disjoint or identical (**Th. 14 on P. 152**). Hence it follows that the required left coset P is xH.

Therefore xH is the unique left coset which is equal to right coset Hx.

$\therefore \quad Hx=xH \ \forall \ x \in G.$

or $\quad Hx\,x^{-1}=xHx^{-1}$

or $\quad H=xHx^{-1} \ \forall \ x \in G$

So H is a normal sub group by Th. 1.

$\therefore$ **H is a normal sub group of G $\Leftrightarrow$ Hx=xH $\forall$ x $\in$ G.**

Theorm 3. *A sub group H of a group G is a normal sub group of G if and only if the product of two right cosets of H in G is again a right coset of H in G.*

Given. H is a normal sub group.

i.e. $\quad Hx=xH \ \forall \ x \in G$ .. (1)

To prove that the product of two right cosets of H in G is again a right coset.

Let $a, b \in G \Rightarrow ab \in G \Rightarrow Ha, Hb, Hab$ are all right cosets of H in G.

Now $(Ha)\ (Hb)=H(aH)\ b=H\ (Ha)\ b$. by I.

$=H\ Hab=Hab \qquad \because \quad HH=H$

Since $ab \in G$

$\therefore$ Hab is again a right coset.

Hence the product of two right cosets of H in G is again a right coset of H in G.

Converse. Given product of two right cosets of H in G is again a right coset of H in G.

To prove. H is a normal sub group.

Let $x \in G \Rightarrow x^{-1} \in G$ so that Hx and Hx^{-1} are two right cosets of H in G.

Since $e \in H \therefore ex \in Hx$ and $ex^{-1} \in Hx^{-1}$

$\therefore \quad ex\ ex^{-1} \in Hx\ Hx^{-1}$ or $e \in Hx\ Hx^{-1}$ ...(1)

Now product of two right cosets is again a right coset and as such (Hx) (Hx^{-1}) is again a right coset and e belongs to it. But $H=He$ is also a righ. cost of H in G and e belongs to it. Hence e belongs to $Hx\ Hx^{-1}$ which is a right coset by given condition and e belongs to H whlch is also a right coset. But two right cosets are either disjoint or identical (Th. 14 P. 152). Hence the two right cosets (Hx) (Hx^{-1}) and H having a common element e must be identical.

$\therefore \quad Hx\ Hx^{-1}=H \ \forall\ x \in G$

$\Rightarrow h_1 x\ hx^{-1} \in H \ \forall\ x \in G$ and $h, h_1 \in H$.

$\Rightarrow h_1^{-1}(h_1 x h x^{-1}) \in h^{-1} H$ or $\in H$ **(See Note below)**

or $\quad xhx^{-1} \in H \ \forall\ x \in G$ and $\forall\ h \in H$

as $h_1^{-1} h_1 = e$.

Hence H is a normal sub group by def. § 2. P. 401.

Note $h_1 \in H \Rightarrow h_1^{-1} \in H$

$\Rightarrow h_1^{-1} H = H$ by Th. 12 P. 151.

i.e. right and left cosets corresponding to any element $h \in H$ is H *i.e.* $Hh=hH=H$ if $h \in H$.

Theorem 4. *The intersection of any two normal sub groups of a group G is a normal sub group.*

Let H and K be two sub groups of G then $H \cap K$ is also a sub group of G. **(Th. 4 P. 140)**

Hence $a \in H \cap K \Rightarrow a \in H, a \in K$.

H is normal sub group
$\Rightarrow x\ ax^{-1} \in H \ \forall\ x \in G, a \in H.$
K is a normal sub group
$\Rightarrow x\ ax^{-1} \in K \ \forall\ x \in G, a \in K$
} $-A$

Relations in A prove that for $\forall\ x \in G$ and $a \in H \cap K$ we have

$x\ a\ x^{-1} \in H$ and $x\ a\ x^{-1} \in K$

or $\quad x\ a\ x^{-1} \in H \cap K.$

Hence $H \cap K$ is also a normal sub group.

Generalisation of the theorem on intersection of two normal sub groups.

The intersection of any family of normal sub groups of G is again a normul sub group of G.

[See page 141 also] **[Raj. M. Sc. 1967)**

Let $A=\{N_1, N_2, \ldots\}$

$A=\{N_i : N_i \text{ is a normal sub group}\}$

Let $N^*=\cap \{N_i : N_i \in A$ *i.e.* N_i is a normal sub group$\}$

We have to prove that N^* is a normal sub group for which we shall use the criteria of § 2 P. 401.

i.e. $x\,a\,x^{-1} \in N^* \forall\ x \in G$ and $a \in N^*$ ...(1)

Let $a \in N^*$ then by definition of intersection

$$a \in N_i \forall\ N_i \in A.$$

Hence $x\,a\,x^{-1} \in \cap \{N_i : N_i \text{ is a normal sub group}\}$.

or $x\,a\,x^{-1} \in N^* \forall\ x \in G$ and $a \in N^*$.

Therefore N^* is also a normal sub group

Exercise I

Ex. 1. *Prove that every sub group H of an abelian group G is a normal sub group and hence deduce that every sub group of a cyclic group is also normal.*

H will be a normal sub group of G if

$$x\,h\,x^{-1} \in H \forall\ x \in G \text{ and } h \in H.$$

Now $x\,h\,x^{-1}=x\,(h\,x^{-1})=x\,(x^{-1}\,h)$ as G is abelian

$=(x\,x^{-1})\,h=e\,h=h$. which belongs to H.

Since $x\,h\,x^{-1} \in H \forall\ x \in G$ and $h \in H$, it follows that the sub group H is a normal sub group.

Again as every cyclic group is abelian therefore every sub group of a cyclic group is a normal sub group by part I.

Ex. 2. *If H and K are normal sub groups of a group G, show that H K is also a normal sub group of G.*

Here first of all we should prove that $H\,K$ is a sub group of G and then show that $H\,K$ is a normal sub group.

Let $h_1, h_2 \in H \Rightarrow k_1 h_2^{-1} \in H = h$ say

as H is a sub group.

$k_1, k_2 \in K \Rightarrow k_1 h_2^{-1} \in K = k$ say

as K is a sub group. ...(2)

To show that H K is a sub group of G ...(2)

Now $h_1k_1, h_2k_2 \in H\,K$ and it will be a sub group,

if $(h_1k_1)\,(h_2k_2)^{-1} = (h_1k_1)\,(k_2^{-1}\,h_2^{-1})$

$= h_1\,(k_1k_2^{-1})\,h_2^{-1}$

$= (h_1h_2^{-1})\,\{h_2\,(k_1k_2^{-1})\,h_2^{-1}\}$ **(Note this step)**

$= h\,\{h_2\,k\,h_2^{-1}\}$ by 1 and 2

$\in H\,K$ and hence $H\,K$ is a sub group if we show that $h_2kh_2^{-1} \in K$, which is true as K is given to be normal sub group by § 2 P. 401

i e. $x\,hx^{-1} \in H\ \forall\ x \in G$ and $h \in H$.

Now we shall show that **H K is a normal sub group.**

Let $h \in H, k \in K \Rightarrow h\,k \in HK$.

Also H is a normal sub group

$\Rightarrow x\,h\,x^{-1} \in H\ \forall\ x \in G, h \in H$

and K is a normal sub group

$\Rightarrow x\,k\,x^{-1} \in K\ \forall\ x \in G, k \in K$

$\therefore\ (x\,h\,x^{-1})\,(x\,k\,x^{-1}) \in H\,K$

or $x\,h\,(x^{-1}\,x)\,k\,x^{-1} \in H\,K$

or $x\,(h\,k)\,x^{-1} \in H\,K\ \forall\ x \in G, h\,k \in HK$

$\therefore$ $H\,K$ is a normal sub group.

Ex. 3. *If H is a sub group of G and K is a normal sub group of G then prove the following.*

(a) H K is a sub group of G.

We have proved this in part I of Ex. 2. where only the condition of K being normal sub group was used for proving HK to be *a* sub group.

(b) K H is a sub group of G.

Proceeding as is in Ex. 2. we have k_1h_1, k_2h_2 be any two elements of KH,

then $(k_1h_1)\,(k_2h_2)^{-1}=k_1\,h_1\,h_2^{-1}\,k_2^{-1}$

$=[k_1\,(h_1\,h_2^{-1})\,k_2^{-1}]\,h_2\,h_1^{-1}\,h_1\,h_2^{-1}$ **(Not this step)**

$=k_1\,[(h_1\,h_2^{-1})\,k_2^{-1}\,(h_1\,h_2^{-1})^{-1}]\,h_1\,h_2^{-1}$ ...(1)

Now $h_1, h_2 \in H \Rightarrow h_1h_2^{-1} \in H=h$ say as H is a sub group.

$\therefore$ $h_1\,h_2^{-1} \in G$ also as H is a sub group of G

Again since K is a normal sub group of G and $k_2^{-1} \in K$

and $h_1h_2^{-1} \in G$

$\therefore$ $(h_1h_2^{-1})\,k_2^{-1}\,(h_1h_2^{-1})^{-1} \in K=k_3$ say. ...(2)

by $xh\,x^{-1} \in H\ \forall\ x \in G,\ h \in H$

when H is a normal sub group of G by § 2 P. 401.

Now $k_1 \in K$, $k_3 \in K$. (3)

$\therefore$ $k_1k_3 \in K=k$ say, as K is a sub group.

$\therefore$ From I we get by the help of (2) and (3)

$(k_1h_1)\,(k_2\,h_2)^{-1}=k_1\,[k_3]\,h=k_1k_3h=kh$ by (3) $\in K\,H$

Hence $K\,H$ is a sub group.

(c) H ∩ K is normal sub group of H.

Since both H and K are sub groups therefore $H \cap K$ is also a sub group of G.

Again we know that $H \cap K \subset H$ and hence it follows that $H \cap K$ is a sub group of H.

Now H ∩ K will be a normal sub group of H if we show that

$x\,a\,x^{-1} \in H \cap K \;\forall\; x \in H$ and $a \in H \cap K$.

Let $a \in H \cap K \Rightarrow a \in H,\ a \in K$.

Again K is a normal sub group of G

$\therefore \quad x\,a\,x^{-1} \in K \;\forall\; x \in G,\ a \in K$

or $\qquad\qquad \forall\; x \in H,\ a \in H \cap K. \qquad \ldots (1)$

Again since H is given to be a sub group therefore

$a \in H,\ x \in H \Rightarrow ax^{-1} \in H, \Rightarrow x\,a\,x^{-1} \in H$

$\therefore \quad x\,a\,x^{-1} \in H \;\forall\; x \in H$ and $a \in H$

or $\qquad\qquad \forall\; x \in H$ and $a \in H \cap K. \qquad \ldots (2)$

Hence from (1) and (2) we prove that

$x\,a\,x^{-1} \in H \cap K \;\forall\; x \in H$ and $a \in H \cap K$.

Therefore by § 2 P. 401.

$H \cap K$ is a normal sub group of H

(d) K is a normal sub group of HK.

Let $k \in K$ and $e \in H$.

then $k = e\,k \in HK$

$\therefore \quad k \in K \Rightarrow k \in HK \quad \therefore \quad K \subset HK$

Now K is a sub group of G and HK is also a sub group of G by part (a) and $K \subset HK$. therefore K is a sub group of HK.

Now we have to show that K is a normal sub group of HK for which we shall use the criteria

$x\,a\,x^{-1} \in H \;\forall\; x \in G$ and $a \in H$, for H to be a normal sub group of G.

Now $h_1k_1 \in HK,\ k \in K$

$\therefore \quad (h_1k_1)\,k\,(h_1\,k_1)^{-1}$ should be shown to belong to K for proving K to be a normal sub group of HK.

Now $(h_1\,k_1)\,k\,(h_1\,k_1)^{-1} = (h_1\,k_1)\,k\,(k_1^{-1}\,h_1^{-1})$

$= h_1\,(k_1\,k\,k_1^{-1})\,h_1^{-1}$.

$= h_1$ (an element a of K which is a normal sub group) h_1^{-1}.

$= h_1\, a\, h_1^{-1} \in K \;\forall\; h_1 \in G$ and $a \in K$ as K is a normal sub group.

Thus $(h_1\, k_1)\, k\, (h_1\, k_1)^{-1} \in K \;\forall\; h_1\, k_1 \in HK$ and $k \in K$.

$\therefore$ K is a normal sub group of HK.

Ex. 4. *If H and K are normal sub groups of a group G such that $H \cap K = \{e\}$, show that every element of H commutes with every element of K.*

Let $h \in H$ and $k \in K$, where H and K are normal sub groups of G.

Now $h\, k\, h^{-1}\, k^{-1} = (h\ k\, h^{-1})\, k^{-1}$

But $h\, k\, h^{-1} \in K$ as K is normal sub group. Also $k \in K \Rightarrow k^{-1} \in K$

$\therefore$ $(h\, k\, h^{-1})\, k^{-1} \in K$. ...(1)

Again $h\, k\, h^{-1}\, k^{-1} = h\, (k\, h^{-1}\, k^{-1})$

But $k\, h^{-1}\, k^{-1} \in H$ as H is a normal sub group. Also $h \in H$.

$\therefore$ $h\, k\, h^{-1}\, k^{-1} \in H$. ...(2)

Hence $h\, k\, h^{-1}\, k^{-1} \in H \cap K$ by 1 and 2

Since $H \cap K = \{e\}$ given therefore it follows that

$h\, k\, h^{-1}\, k^{-1} = e \Rightarrow h\, k\, h^{-1}\, k^{-1}\, k = e\, k$

$\Rightarrow h\, k\, h^{-1} = k \Rightarrow h\, k\, h^{-1}\, h = kh.$

$\Rightarrow hk = kh$

Hence every element of H commutes with every element of K.

Ex. 5. *Prove that a normal sub group is commutative with every complex.*

Let H be a complex and K be a normal sub group

Let $h \in H$ and H being a complex is a sub set of G.

$\therefore$ $h \in H \Rightarrow h \in G \Rightarrow h^{-1} \in G$ and $h\, h^{-1} = e$. Choose $k \in K$.

We have to prove that $HK = KH$.

Now $hk \in HK$ but $hk = h\, k\, h^{-1}\, h$

$=(h\ k\ h^{-1})\ h=$(some element of K) $h \in H$.

$\because$ K being a normal sub group.

$\Rightarrow h\ k\ h^{-1} \in K\ \forall\ h \in G$ and $k \in K$

$\therefore\ \ h\ k \in H\ K \Rightarrow h\ k \in KH$

$\therefore\ \ H\ K \subset K\ H$ ...(1)

Again $k\ h \in KH$

But $kh=h\ h^{-1}\ kh=h\ (h^{-1}\ k\ h)$

$=h$ (some element of K) $\in H\ K$

Because K being a normal sub group

$\Rightarrow h^{-1}\ k\ h \in K\ \forall\ h^{-1} \in G$ and $k \in K$.

Since $kh \in KH \Rightarrow k\ h \in HK$

$\therefore\ \ K\ H \subset HK.$ ...(2)

From 1 and 2 we conclude that $H\ K=K\ H$.

i.e. a normal sub group K of G commutes with every complex H of G.

Ex. 6. *Prove that a sub group H of index 2 in a group G is a normal sub group of G.*

Refer P. 160. The index of a subgroup H of G is equal to the number of distinct right (left) cosets of H in G.

Also we know that

$G=H \cup H\ a \cup H\ b \cup H\ c$ ..**Cor 1 P. 153**

$=H \cup a\ H \cup b\ H \cup c\ H$...

where all the cosets are distinct.

Here the index of sub group H in G is 2 and as such the number of distinct right (left) cosets of H in G is 2.

Let x be any element of G then it may or may not belong to H.

If $x \in H$ then we know that $Hx=H$ and $xH=H$.

Th. 12. P. 152

Thus $Hx=xH$. if $x \in H$.

If $x \notin H$ then the right cosets Hx and H are distinct

and there will be only two distinct cosets, Similarly the left cosets xH and H will be distinct. H is both a right and left coset.

$$\therefore \quad G=H \cup Hx=H \cup xH. \qquad \ldots(1)$$

But no elements are common in H and Hx, and also in H and xH for otherwise they will no be distinct.

Hence from (1) it follows that $Hx=xH$, if $x \in G$ but $x \notin H$,

Therefore $Hx=xH \ \forall \ x \in G$ and as such H is a normal sub group by Th. 2 **P. 404.**

Ex. 7. *If H is a normal sub group of a group G and K is sub group of G such that $H \subset K \subset G$., prove that H is also a normal sub group of K.*

H being a sub group of G and K is also a sub group of G and $H \subset K$, it follows that H is a sub group of K.

Now H will be a normal sub group of K if .. (1)

$$Hx=xH \ \forall \ x \in K$$

Above relation clearly holds good as it holds good $\forall \ x \in G$

i e. $Hx=xH \ \forall \ x \in G$, H being normal sub group.

Hence relation I is true and as such H is normal sub group of K.

Ex 8. *If H be the only sub group of finite order m in group G, prove that H is a normal sub group of G,*

$o\,(H)=m$ given and H is a sub group.

$$\therefore \quad H=\{h_1, h_2, \ldots, h_m\}$$

$\therefore$ $x\,Hx^{-1}$ is also a sub group $\forall \ x \in G$ **See Ex. 6 P. 139**

$$x\,H\,x^{-1}=\{x\,h_1\,x^{-1}, x\,h_2\,x^{-1}, \ldots, x\,h_m\,x^{-1}\}$$

All the elements are distinct for if not let $xh_i\,x^{-1}=xh_jx^{-1}$

$\Rightarrow h_i=h_j$ which is not true as $o\,(H)=m$ given

$\therefore \quad o(x H x^{-1}) = m.$

But H is the only sub group of order m.

$\therefore \quad x H x^{-1} = H. \ \forall \ x \in G.$

Hence H is a normal sub group by Th. 1 P. 402.

Ex 9. *If H is a sub group of G, let $N(H) = \{x \in G : xHx^{-1} = H\}$, then prove the following*

(*a*) *$N(H)$ is a sub group of G.*

(*b*) *H is a normal sub group of $N(H)$*

(*c*) *If H is a normal sub group of the sub group K in G then $K \subset N(H)$*
i.e. $N(H)$ is the largest sub group of G in which H is normal

(*d*) *H is normal in G if and only if $N(H) = G$.*

(a) **N (H) is a sub group of G.**

$N(H) = x \in G : x H x^{-1} = H\}$.

Let $a, b \in N(H) \Rightarrow a H a^{-1} = H, b H b^{-1} = H.$

$\Rightarrow b^{-1} (b H b^{-1}) b = b^{-1} H b.$

$\Rightarrow H - b^{-1} H b.$ ...(1)

$N(H)$ will be sub group of G if we show that

$$ab^{-1} \in N(H)$$

Now $ab^{-1} H (ab^{-1})^{-1} = (ab^{-1}) H (b a^{-1})$

$= a \{b^{-1} H b) a^{-1} = a H a^{-1} = H$ by *I*.

Above relation shows that $a \ b \in N(H) \Rightarrow ab^{-1} \in N(H)$ and hence $N(H)$ is a sub group.

(b) **H is normal sub group of N (H).**

First we show that H is a sub group af $N(H)$

Let $h \in H$ then $h H h^{-1} = H$ which shows that

$$h \in N(H)$$

$\therefore \quad H \subset N(H)$ and as such H is a sub group of $N(H)$

Again $\forall \ x \in N(H)$ we have $xHx^{-1} = H$ and hence by Th. 1 p 401 H is normal sub group of $N(H)$.

(c) **If H is normal sub group of K then**

$\forall \ x \in K$ we have $x H x^{-1} = H$ by Th. 1 P. 401

Above relation shows that $x \in N(H)$

$\therefore \quad x \in K \Rightarrow x \in N(H) \qquad \therefore \quad K \subset N(H).$

(d) Let H be normal in $G \Rightarrow \forall \ x \in G$ we have
$x H x^{-1} = H$ **Th. 1 P. 401** $\therefore \quad x \in N(H).$

$\therefore \quad G \subset N(H)$. But $N(H) \subseteq G$ by def. of $N(H)$.

$\therefore \quad N(H) = G$

Conversly Let $N(H) = G$.

$\therefore \quad x \in G \Rightarrow x \in N(H) \Rightarrow x H x^{-1} = H \ \forall \ x \in G$

$\therefore \quad H$ is normal sub group of G.

§ **4. Simple Group.**

Proper and improper normal sub groups of a group G.

Every group G has at least two normal sub groups which are the group G itself and the sub group consisting of identity element alone. These two normal sub groups are called improper normal sub groups of group G. All other normal sub groups of G other than the above two will be called proper normal sub groups.

Smiple groups : *A group G having no proper sub groups is called a simple group.*

In other words a group G whose only normal sub groups are G and the identity element e will be called a simiple group.

As an illustration we can say that a group G of prime order p is simple. By Lagranges theorem we know that order of a sub group H of a finite group G is a divisor of the order of group § **11 P 161.** Since order of group G is prime therefore its only two sub groups will be either G itself or sub group consi sting of identity element which are improper sub groups *i.e.* it has no proper sub groups. Hence the group will be a simiple group-

§ **5. Relation of conjugacy in a group G.**

Def. *An element $a \in G$ will be conjugate to an element $b \in G$ expressed $a \ a \sim b$ if there exists some x in G*

such that $a=x^{-1}bx$ and this relation is called relation of conjugacy.

Theorem 5. *The relation of conjugacy in a group G is an equivalence relation.*

We have to prove that the relation of conjugacy is

(1) Reflexive (2) Symmetric (3) Transitive.

Reflexive. Let a be any element of G then there exists e in G such that

$a=e^{-1}\,a\,e$ and hence by definition $a \sim a$.

Symmetric. Let $a \sim b$ and we shall show that $b \sim a$.

Since $a \sim b \Rightarrow a=x^{-1}\,bx$ for x in G

$\Rightarrow x\,a\,x^{-1}=x\,(x^{-1}\,bx)\,x^{-1} \Rightarrow (x^{-1})^{-1}\,ax^{-1}=b$

Since $x \in G$ therefore $x^{-1} \in G$ and let $x^{-1}=k$.

$\therefore\ b=k^{-1}\,a\,k,\ k \in G \Rightarrow b \sim a$.

Transitive. $a \sim b,\ b \sim c \Rightarrow a \sim c$

Since $a \sim b \Rightarrow a=x^{-1}\,b\,x$ for some x in G

$b \sim c \Rightarrow b=y^{-1}\,c\,y$ for some y in G.

Putting for b in Ist relation we get

$$a=x^{-1}\,(y^{-1}\,cy)\,x=x^{-1}\,y^{-1}\,(c)\,y\,x.$$

$$=(y\,x)^{-1}\,c\,(y\,x).\ y\,x \in G \text{ as } x, y \in G$$

$$\therefore\ a \sim c.$$

Hence the relation of conjugacy is an equivalence rela-

ol .

It will partition the group G into disjoint equivalence classes known as **classes of conjugate elements** such that

(*a*) Any two elements of the same class are conjugate.

(*b*) No two elements of different classes are conjugate.

Conjugate class of an element a : This class will consist of all those elements of G which are conjugate to a and will be denoted by a or $C\,(a)$

$$\therefore\ a \text{ or } C\,(a)=\{x \in G : x \sim a\}.$$

It will consist of elements of the type $x^{-1} a x$ as x ranges over G. The number of elements in $C(a)$ will be denoted by C_a, whenever G is a finite group.

§ 6. Normalizer of an element of a group.

Definition. *The set of all those elements of a group G which commute with a fixed element a of a group G is called normalizer of an element a of the group and is denoted by* $N(a)$

$$N(a)=\{x \in G : a\, x=x\, a\},$$

Theorem 6. *The normalizer $N(a)$ of an element $a \in G$ is a sub group of G.*

We have already proved this theorem in Ex. 3 P. 137.

Particular Cases.

(a) Normalizer N (e) of element e of G is G is itself.

$$N(e)=\{x \in G : xe=e\, x\}=G.$$

as $$x\, e=e\, x \;\forall\; x \in G.$$

(b) Normalizer N (a) of an element a of an abelian group is G itself.

$$N(a)=\{x \in G : x\, a=a\, x\}=G$$

as $$x\, a=a\, x \;\forall\; x \in G \text{ when } G \text{ is abelian.}$$

(c) Normalizer N (a) is not necessarily a normal sub group.

We have proved that $N(a)$ is a sub group and let us denote it by H *i.e.* $N(a)=H$.

If $h \in N(a)$ *i e.* H then $h\, a=a\, h$. .. (1)

Now $N(a)$ or H will be normal sub group if

$x\, h\, x^{-1} \in H$ *i.e.* $N(a)$ for every $x \in G$ and $h \in H$.

Further we must establish that

$$(x\, h\, x^{-1})\, a=a\, (x\, h\, x^{-1})$$

which is not necessarily true by the help of (1).

It will however be true if the group be abelian for in that case

$$(x\, h\, x^{-1})\, a=x\, h\, (x^{-1}\, a)=x\, h\, (a\, x^{-1})=x\, (h\, a)\, x^{-1}$$

$$=x\ (a\ h)\ x^{-1}=(x\ a)\ h\ x^{-1}=(a\ x)\ h\ x^{-1}$$
$$=a\ (x\ h\ x^{-1}).$$

Theorem 7. *Let a be any element of a group G. The two elements $x, y \in G$ give rise to the same conjugate of a if and only if they belong to the same right coset of the normalizer $N(a)$ of a in G.*

Method. We shall show that if x and y belong to the same right coset of sub group $N(a)$ of a in G then they give the same conjugate of a whereas, if they belong to different right cosets of sub group $N(a)$ of a in G then they give different conjugates of a.

Proof. Referring to Theorem 15 P. 153 we have

$$H\,a=H\,b \Leftrightarrow ab^{-1} \in H.$$

Now we know that $x \in H\,x, y \in H\,y.$ **(Ex. 3 P. 150)**

But if x, y belong to the same right coset Hx of sub group H in G then $x \in H\,x, y \in H\,x$ but $y \in H\,y$.

$\therefore$ $H\,x$ and $H\,y$ have y common and as such they must be identical as the two right cosets are either disjoint or identical.

$\therefore$ $H\,x=H\,y$ and hence $x\,y^{-1} \in H$

Now let $x, y \in$ to same right coset of sub group $N(a)$ in G.

Therefore $x\,y^{-1} \in$ to $N(a)$ as shown above.

$\therefore$ $a\ (x\,y^{-1})=(x\,y^{-1})\ a$ by definition of $N(a)$

$\Rightarrow x^{-1}\ (a\ x\ y^{-1})\ y=x^{-1}\ (x\ y^{-1}\ a)\ y.$

$\Rightarrow x^{-1}\ a\ x=y^{-1}\ a\ y.$

Above relation shows that x and y give rise to the same conjugate of a.

2nd part. Now let us suppose that x, y belong to different right cosets of $N(a)$ in G then we shall show that they cannot give rise to same conjugate of a.

i.e. $x^{-1}\ a\ x \neq y^{-1}\ a\ y.$

If possible let $x^{-1} a x = y^{-1} a y$.

$$\therefore \quad x (x^{-1} a x) y^{-1} = x (y^{-1} a y) y^{-1}$$

or $$a x y^{-1} = x y^{-1} a \Rightarrow x y^{-1} \in N (a).$$

But $x y^{-1} \in N (a)$ implies that x, y belong to the same right coset of $N (a)$ as shown in first part which is a contradiction to the supposition that x, y belong to different right cosets of $N (a)$ in G.

Hence $x^{-1} a x \neq y^{-1} a y$ *i.e.* x, y cannot give rise to same conjugate of a.

Theorem 8. *If G is a finite group, then the number of elements in the class $C (a)$ of elements conjugate to a is the index of the normalizer of a in G i.e. index of sub group $N (a)$. In other words.*

$$C_a = \frac{o (G)}{o (N (a))}.$$

By definition we know that

$C (a) = \{x^{-1} a x : x \in G\}$ or $= \{x \in G : x \sim a\}$

C_a = number of elements in $C (a)$.

Also $N (a) = \{x \in G : a x = x a\}$

where $N (a)$ is a sub group.

Denote by A the set of all right cosets of sub group $N (a)$ in G.

$$\therefore \quad A = \{N (a) x : x \in G\}.$$

Also index of sub group H of $G = \frac{o (G)}{o (H)}$.

Let us define a mapping from the set of right cosets of $N (a)$ in G and the elements conjugate to a.

i.e. $f : A \to C (a)$ such that

$$f [N (a) x] = x^{-1} a x \ \forall \ x \in G.$$

The above mapping is well defined *i.e.* independent of he selection of right cosets.

i.e. if $N(a)\,x = N(a)\,y$ then $f[N(a)\,x] = f[N(a)\,y]$.

Now if $N(a)\,x = N(a)\,y$. Then from Theorem 15 Page 153 *i.e.* $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Hence from $N(a)\,x = N(a)\,y$ we get $xy^{-1} \in N(a)$.

$\therefore$ $a(x\,y^{-1}) = (x\,y^{-1})\,a$ by definition of $N(a)$

or $x^{-1}(a\,x\,y^{-1})y = x^{-1}(x\,y^{-1}\,a)\,y$ or $x^{-1}\,a\,x = y^{-1}\,a\,y$

or $f[N(a)\,x] = f[N(a)\,y]$.

Hence the mapping f is well defined.

Now we shall prove that this mapping is **one-one onto.**

f is one-one

Let $f[N(a)\,x] = f[N(a)\,y]$

$\Rightarrow x^{-1}\,a\,x = y^{-1}\,a\,y$ by def. of f.

$\Rightarrow x(x^{-1}\,a\,x)\,y^{-1} = x(y^{-1}\,a\,y)\,y^{-1}$

$\Rightarrow a\,x\,y^{-1} = x\,y^{-1}\,a$.

$\Rightarrow a(x\,y^{-1}) = (x\,y^{-1})\,a$.

$\Rightarrow x\,y^{-1} \in N(a)$ by def. of $N(a)$.

$\Rightarrow N(a)x = N(a)\,y$.

$\because$ $Ha = Hb \Leftrightarrow ab^{-1} \in H$.

Hence f is one-one.

f is onto. Let $x^{-1}\,a\,x$ be any element of $C(a)$ where $x \in G$ then $N(a)\,x$ is a coset of sub group $N(a)$ in G corresponding to $x \in G$ such that $f[N(a)\,x] = x^{-1}\,a\,x$. Thus every element of $C(a)$ is the f-image of an element of A.

Therefore $f: A \to C(a)$ is an onto mapping.

Above relation establishes a one-one correspondence between the right cosets of $N(a)$ in G and the elements of $C(a)$ *i e.* conjugate of a.

Hence if G be a finite group, then

C_a = number of distinct elements in $C(a)$

= number of distinct right cosets of sub group $N(a)$ of G

$$= \text{index of sub group } N(a) \text{ of } G$$

$$= \frac{o(G)}{o(N(a))} \text{ by def. of index of a sub group.}$$

Cor. I. P. 162.

§ 7. Self Conjugate elements.

We know that $C(a) = \{x \in G : x \sim a\}$.

i.e. it consists of elements of the type $x^{-1}ax \ \forall \ x \in G$.

Now if $C(a)$ consists of only one element *i.e.* a alone then in that case a will be a **self conjugate element** and we will have

$$a = x^{-1} a x \ \forall \ x \in G$$

or $$x a = a x \quad \forall \ x \in G.$$

or a **commutes with every element of the group.** if a is self conjugate element which is also sometimes called invariant element.

Definition. *An element $a \in G$ is said to be self conjugate if the class $C(a)$ of elements conjugate to a consists of a alone i.e. $C(a) = \{a\}$.*

§ 8. Centre of a group

Definition. *The set Z of all self conjugate elements of a group G is called the centre of G i.e.*

$$Z = \{z \in G : zx = xz \ \forall \ x \in G\}.$$

By definition self conjugate element of G is one which commutes with every element of G.

Theorem 9. *The centre Z of a group G is a normal sub group of G.*

Note. Compare this theorem with Theorem 6 on Page 417 $N(a) = \{x \in G : a x = x a\}$ is a sub group of G.

The difference between elements of Z and $N(a)$ should be noted.

The elements of centre Z commute with every element of G whereas elements of $N(a)$ the normalizer of an element a commute with a only.

The centre Z will be proved to be normal sub group, whereas $N(a)$ was only a sub group.

Proof. Centre of Z is a sub group.

Let $z_1, z_2 \in Z$, then Z will be a sub group if

$$z_1 z_2^{-1} \in Z \qquad \textbf{Th. 2 P. 132.}$$

$$z_1 \in Z \Rightarrow z_1 x = x z_1 \quad \forall\ x \in G$$

$$z_2 \in Z \Rightarrow z_2 x = x z_2 \quad \forall\ x \in G.$$

Now $z_2 x = x z_2 \Rightarrow z_2^{-1}(z_2 x) z_2^{-1} = z_2^{-1}(x z_2) z_2^{-1}$

$$\Rightarrow x z_2^{-1} = z_2^{-1} x \ \forall\ x \in G \Rightarrow z_2^{-1} \in Z.$$

We shall now show that $z_1 z_2^{-1} \in Z$.

$$x(z_1 z_2^{-1}) = (x z_1) z_2^{-1} = (z_1 x)(z_2^{-1}) \quad \because \quad z_1 \in Z$$

$$= z_1 (x z_2^{-1}) = z_1 (z_2^{-1} x) \quad \therefore \quad z_2^{-1} \in Z$$

$$= (z_1 z_2^{-1}) x.$$

Since $x(z_1 z_2^{-1}) = (z_1 z_2^{-1}) x \quad \forall\ x \in Z.$

is follows that

$$z_1 z_2^{-1} \in Z \quad \text{whenever } z_1, z_2 \in Z.$$

Hence Z is a sub group of G.

Z is a normal sub group.

Let $z \in Z \Rightarrow z x = x z \ \forall\ x \in G.$

$$\therefore \quad x z x^{-1} = (x z) x^{-1} = (z x) x^{-1} = z \in Z.$$

$$\therefore \quad z \in Z, x \in G \Rightarrow x z x^{-1} \in Z$$

and hence by definition Z is a normal sub group.

Theorem 11. *If Z be the centre of a group G and $a \in G$. then $a \in Z$ if and only if $N(a) = G$. If G is finite then $a \in Z$ if and only if $o(N(a)) = o(G)$.*

$$Z = \{z \in G : x z = z x \ \forall\ x \in Z\}$$

$$N(a) = \{x \in G : a x = x a\}.$$

If $a \in Z$ then $a x = x a \quad \forall\ x \in G.$

Since for all $x \in G$ we have $a x = x a$, therefore $N(a) = G$. On the other hand

$$N(a) = G \Rightarrow a x = x a \ \forall\ x \in G$$

$$\Rightarrow a \in Z.$$

Again if G be finite then

$$N(a)=G \Leftrightarrow o(N(a))=o(G).$$

Hence $a \in Z \Leftrightarrow N(a)=G \Leftrightarrow o(N(a))=o(G)$.

§ 9. Certain Definitions.

(a) Cynjugate sub groups.

We have defined conjugate elements a and b in a group G.

i.e. $a=x^{-1} b x$ for some $x \in G$ then a is said to be conjugate to b, and that the relation of conjugacy in a group G is an equivalence relation.

In a similar manner we can define conjugate sub groups.

Definition. *Let A and B be two subgroups of a group G then A is said to be a conjugate to B if the e exists an x in G such that $A=x^{-1} B x$ and then we write it as $A \sim B$.*

Theorem 10. *The relation of conjugacy is an equivalence relation in the set of all sub groups of a group G.*

We can prove as in Th. 5 P. 416.

(b) Normalizer of a sub group of a group.

We have defined normalizer of an element a of a group G *i.e.* $N(a)$ the set of all those elements of a group G which commute with a.

i.e. $N(a)=\{x \in G : a x=x a\}$

Also we have proved that $N(a)$ is a sub group.

Definition. *Similarly if A is a sub group of a group G then $N(A)$ the normalizer of A in G is the set of all those elements of G which commute with A.*

i.e. $N(A)=\{x \in G : x A=A x\}$.

It can be proved as in Th. 6 P. 417 that the nomalizer $N(A)$ of a sub group A of a group G is a sub group of G.

(c) Self Conjugate sub groups.

We have defined self conjugate elements of a group G as an element a if $C(a)=\{a\}$. *i.e.* $a=x^{-1} a x \ \forall \ x \in G$.

or $$x\,a = a\,x \;\forall\; x \in G.$$

Similarly *a* sub group A of a group G is said to be self conjugate if A is the only sub group belonging to the class $C(A)$ of sub groups which are conjugate to A.

Hence A is self conjugate sub group.

iff $A = x^{-1} A x$ or $x A = A x$. $\forall\; x \in G$.

§ 10. Quotient Groups.

Let H be a normal sub group of group G and Ha, $a \in G$ be right coset of H in G. Now the sub group H being normal the left coset aH will be same as the right coset Ha. Thus we shall simply say that Ha is a coset of normal sub group H in G.

The set of all cosets of a normal sub group H in G is denoted by G/H.

Multiplication of cosets of a normal sub group H in G.

Let $a, b \in G$ and Ha, Hb be any two cosets of H in G then

$$(Ha)(Hb) = H(aH)b = H(Ha)b \qquad \because\; aH = Ha$$
$$= HH(ab) = Hab \qquad \because\; HH = H.$$

Since $a, b \in G \Rightarrow ab \in G$ and hence Hab is again a cosect $\in G/H$.

Theorem 12. *The set of all cosets of a normal sub-group is a group with respect to multiplication of complexes as a composition.* **(Raj. M. Sc. 67, 69; Meerut M. Sc. 69)**

Let H be a normal sub group and the set of all cosets of H in G be

$$G/H = \{ Ha : a \in G \}.$$

To prove that G/H is a group for multiplication.

Axioms of groups.

(1) Closure property. The product of two cosets is again a coset $\in G/H$ as proved above. [Reproduce here].

(2) **Associative.** Let $a, b, c \in G$ so that

$$H\,a, H\,b, H\,c \in G/H.$$

$$H\,a\,[(H\,b)\,(H\,c)] = H\,a\,(H\,b\,c) = H\,a\,(b\,c)$$

$\because H\,a . H\,b = Hab$

$$= H\,(a\,b)\,c = (H\,a\,b)\,(H\,c) \text{ by associativity in } G$$

$$= [(H\,a)\,(H\,b)]\,H\,c.$$

Therefore multiplication of cosets in G/H is associative.

(3) **Identity.** Now $H = H\,e$.

$\therefore$ $H.(H\,a) = (H\,e)\,(H\,a) = H\,(e\,a) = H\,a$

$(H\,a).H = (H\,a)\,(H\,e) = H\,(a\,e) = H\,a$

$\because$ $a\,e = a = e\,a$.

Hence the coset H is the identity element $\in G/H$.

Inverse. $a \in G \Rightarrow a^{-1} \in G$

$\therefore$ $H\,a \in G/H \Rightarrow H\,a^{-1} \in G/H$.

Now $(H\,a)\,(H\,a^{-1}) = H\,(a\,a^{-1}) = H\,e = H$

$(H\,a^{-1})\,(H\,a) = H\,(a^{-1}a) = H\,e = H$.

Hence the coset $H\,a^{-1}$ is the inverse of coset $H\,a$.

Therefore G/H is a group w.r.t. multiplication of cosets.

If H be not a normal sub group i.e. H a $\neq$ a H.

It may be clearly understood that the set of right cosets of H in G will not form a group if H were not a normal sub group because in proving closure property we have used the fact $H\,a = a\,H$ which is true only if H were a normal sub group.

(Meerut M. Sc. 69)

Quotient Group.

Definition. *The set G/H of all cosets of a normal sub group H is a group w. r. t. multiplication of cosets and this group is called* **Quotient group or factor group.**

Cor. I. *If G be abelian then quotient group G/H is also abelian where H is a normal sub group.*

$a, b \in G \Rightarrow a\,b = b\,a$ as G is abelian

$$H\,a, H\,b \in G/H \Rightarrow (H\,a)\,(H\,b) = H\,a\,b = H\,b\,a$$

$$= (H\,b)\,(H\,a)$$

Hence G/H is also abelian.

Cor II $o\left(\frac{G}{H}\right)=\frac{o(G)}{o(H)}$

where G is a finite group and H is a normal sub group of G.

Let $o(G)=n$ and order of sub group H be m.

Also if k be number of distinct right cosets of H in G then as discussed in Lagranges Theorem § 11 P. 161 we have

$$n=m\ k \quad \text{or} \quad k=\frac{n}{m}.$$ **Hence proved.**

Cor. III. *The order of $H a \in G/H$ is a divisor of n where n is the order of $a \in G$. H being a normal sub group.*

$$o(a)=n \Rightarrow a^n=e$$

$\therefore$ $H a^n=H e=H$ the identity of G/H.

or $H(a.a.a.....a)=H$

or $(H a)(H a)\ldots\ldots(H a)=H$

or $(H a)^n=H=$identity of G/H.

Now order of $H a$ in G/H is given to be m and also $(H a)^n=H$ therefore m must be a divisor of n.

Cor. IV. *If G be a cyclic group then quotient group G/H is also cyclic.*

Let a be a generator of the cyclic group G and H be any sub group of G.

Now we know that every cyclic group is abelian and every sub group H of an abelian group is normal.

$\because$ $a h a^{-1}=a a^{-1} h=e h=h \in H.$

as G is abelian $\Rightarrow a^{-1} h=h a^{-1}$

Since $a \in G, h \in H \Rightarrow a h a^{-1} \in H$. $\therefore$ H is normal

Hence G/H where H is normal sub group is a quotient group and in order to prove it to be cyclic we have to show that it is generated by some element of G/H.

Now G being cyclic $\Rightarrow a^n \in G \Rightarrow H a^n \in G/H$.

But $H a^n H=(a.a.a.a\ldots\ldots) \in G/H$

$=(H a)\ (H a)\ (H a)\ldots\ldots \in G/H$

$=(H a)^n$

$\therefore\quad H a^n \in G/H=(H a)^n$

Hence G/H is cyclic and is generated by $H a$.

§ 11. Sub group generated by a sub set of a group,

Definition. *Let M be an arbitrary sub set of a group G, then a sub group H of G is called the smallest sub group of G containing H if*

(a) H contains M.

(b) H is contained in every sub group of G which contains M.

In that case H the smallest sub group containing M is called the group generated by M and is denoted by $\{M\}$.

Theorem 13 *Let M be any sub set of a group G then the smallest sub group of G containing M exists and is unique.*

Let $\{M\}$ be the smallest sub group of G containing M.

Choose $F=\{Mi : Mi$ is a sub group of G containing $M\}$.

Clearly F is non empty as G which is a sub group of G containing M belongs to it.

If $H=\cap\ Mi$ then H is also a sub group of G see p. 141.

Clearly H contains M as each Mi contains M.

Again if K be any other sub group of G containing M then K is a member of F and since H is the intersection of members of F it follows that $H \subseteq K$.

i.e. H is contained in every sub group of G which contains M.

Therefore by definition $H=\{M\}$ *i.e.* H is the smallest sub group of G containing M.

Now if H_1 and H_2 be two smallest sub group of G containing M then $H_1 \subset H_2$ as H_1 is smallest sub group therefore it is contained in every other sub group of G which contains M.

Similarly since H_2 is smallest sub group containing M we have as above $H_2 \subset H_1$.

Hence $H_1 = H_2$ thus proving that the smallest sub group containing M is unique.

§ 12. Commutator sub group of a group.

Commutator.

Let G be a group and $x, y \in G$, then the element $xy\, x^{-1}\, y^{-1}$ is called the commutator of the ordered pair (x,y).

Also $(xy\, x^{-1}\, y^{-1})^{-1} = y\, x\, y^{-1}\, x^{-1}$ $\because$ $(y^{-1})^{-1} = y$.

Commutator of ordered pair $(y, x) = yx\, y^{-1}\, x^{-1}$ = Inverse of the commutator of ordered pair (x, y).

Commutator sub group of G.

Let $M = \{xy\, x^{-1}\, y^{-1} : x, y \in G\}$

and G' be the sub group of G generated by M *i.e.* $G' = \{M\}$ then G' is called commutator [sub group of G *i.e.* G' is the smallest sub group of G containing M.

Theorem 14 *Let G be a group and G' be the commutator sub group of G i.e. G' is a sub group generated by M where*

$M = \{xy\, x^{-1}\, y^{-1} : x, y \in G\}$ *then*

(*i*) *G' is a normal sub group of G.*

(Meerut M. Sc. 1969)

(*ii*) *The quotient group G/G' is abeliam.*

(Meerut M. Sc. 1969)

(*iii*) *If H is any normal sub group of G then G/H is abelian $\Rightarrow$ $G' \subset H$.*

(iv) H is a sub group of G and $G' \subset H \Rightarrow$ H is a normal sub group.

Both (iii) and (iv) can be put as under.

If H is any normal sub group of G then G/H is abelian if and only if $G' \subset H$.

Proof. G′ is a normal sub group of G.

(i) Let $\alpha \in G'$ then G' will be normal if

$$x \in G, \alpha \in G' \Rightarrow x \alpha x^{-1} \in G'.$$

Now $x \alpha x^{-1} = x \sigma x^{-1} \alpha^{-1} \alpha = (x \alpha x^{-1} \alpha^{-1}) \alpha \in G'$.

because $x \alpha x^{-1} \alpha^{-1} \in G'$ and $\alpha \in G$.

Hence G' is a normal sub group of G.

(ii) Quotient group G/G′ is abelian.

Let a and b be any two elements of G then $G'a$ $G'b$ are any two elements of quotient group G/G'. We have to prove that G/G' is abelian

Now $ab\,a^{-1}\,b^{-1} \in M \Rightarrow a\,b\,a^{-1}\,b^{-1} \in G' \quad \because M \subset G'$

$$\Rightarrow (a\,b)\,(b\,a)^{-1} \in G'$$

$$\Rightarrow G'\,(a\,b) = G'\,(b\,a) \qquad \because Ha = Hb \Rightarrow ab^{-1} \in H$$

$$\Rightarrow (G'\,a)\,(G'\,b) = G'\,(b)\,G'\,(a) \qquad \because HaHb = Hab$$

$\Rightarrow G'G'$ is abelian.

(iii), (iv) Let H be any normal sub group of G and $a, b \in G$ then Ha, Hb are any two elements of G/H.

Ist Case. G/H is abelian, to prove $G' \subset H$

$$(H\,a)\,(H\,b) = (H\,b)\,(H\,a).$$

$\Rightarrow Ha\,b = Hb\,a \Rightarrow (a\,b)\,(b\,a)^{-1} \in H.$

$\Rightarrow a\,b\,a^{-1}\,b^{-1} \in H \Rightarrow M \subset H$ as $a\,b\,a^{-1}\,b^{-1} \in M$.

Hence H is a sub group of G which contains M. But G' is the smallest sub group of G which contains M, hence G' must be contained in H *i e.* $G' \subset H$.

2nd Case. $G' \subset H$ but $M \subset G'$

$\therefore$ $M \subset H \Rightarrow a\,b\,a^{-1}\,b^{-1}$ belonging to M also belongs to H.

or $a\,b\,a^{-1}\,b^{-1} \in H \Rightarrow (a\,b)\,(b\,a)^{-1} \in H$

$\Rightarrow H(a\,b) = H(b\,a) \Rightarrow H(a)\,H(b) = H(b)\,H(a)$

$\Rightarrow G/H$ is abelian.

CHAPTER VI

GROUP HOMOMORPHISM

§ 1. Definitions.

(a) Homomorphism onto.

A mapping f from a group G onto a group G′ is called homomorphism of G′ if $\forall\ a, b \in G$

$$f(a.b) = f(a).f(b). \qquad \ldots (1)$$

In this case the group G' is said to be **homomorphic image** of group G or else the group G is said to homomorphic to group G'. Symbolically we say $G \simeq G'$. It may be noted that for isomorphism we use the symbol $\cong$ *i e.* $G \cong G'$ and for homomorphism we use the symbol $\simeq$. On the left hand side of (1) the dot. denotes multiplication composition in G whereas on the right it denotes the multiplication composition in G'.

Distinction between isomorphism and homomorphism. The isomorphic mapping should be necessarily one-one and onto satisfying the above condition I, whereas a homomorphic (onto), mapping need not be necessarily one-one. It may be many one.

Again we know that the relation of isomorphism in the set of groups is an equivalence relation but the relation of homomorphism will not be an equivalence relation. Because the relation of homomorphism will not be symmetric as we know that only one-one onto mappings are invertible. In other words $G \simeq G'$ does not imply $G' \simeq G$ where as

$$G \cong G' \Rightarrow G' \cong G.$$

(b) Homomorphism into

A mapping f from a group G into a group G' is called homomorphism of G into G' if $\forall\ a, b \in G$

$$f(a.b)=f(a)\ f(b). \qquad \ldots(1)$$

In this case G' will not be said to be homomorphic image of G but we will show later that homomorphic image of G which will be $f(G)$ to be a sub group of group G'.

(c) Endomorphism.

A homomorphism of a group into itself is called on endomorphism.

§ 2. Certain properties of homomorphism.

(1) *If f is a homomorphism of a group G onto (into) a group G' then $f(e)=e'$ where e and e' are the identities of G and G' respectively.*

i.e. the zero's correspond.

Let $a \in G$ so that $f(a) \in G'$

Then $f(a).e'=f(a)$ as e' is identity of G'

$=f(a.e)$ as e is identity of G

$=f(a)\ f(e)$ by (1)

$\therefore\ f(a).e'=f(a).f(e)$

But G' is a group and hence by cancellation law we have

$$f(e)=e'.$$

(2) *The image of inverse of $a \in G$ is inverse of the image of a*

i.e. $f(a^{-1})=[f(a)]^{-1}$

$a \in G \Rightarrow a^{-1} \in G$ and $a\,a^{-1}=e$

$\Rightarrow f(a\,a^{-1})=f(e)$

$\Rightarrow f(a)\ f(a^{-1})=e'$ $\quad \because f(e)=e'$

$\Rightarrow f(a^{-1})$ is the inverse of $f(a) \in G'$

or $f(a^{-1})=[f(a)]^{-1}$

(3) *If the order of $a \in G$ is finite say n then the order of $f(a)$ i.e. m is a divisor of n.*

$$o(a)=n \Rightarrow a^n=e$$
$$\therefore\quad f(a^n)=f(e) \Rightarrow f(a.a.a\ldots\ldots)=e'$$
$$\Rightarrow f(a)\,f(a)\,f(a)\ldots\ldots=e'$$
$$\Rightarrow [f(a)]^n=e'$$

Hence if m is the order of $f(a)$ in G' then m must be a divisor of n.

(4) Homomorphic image of an abelian group is abelian

Let $a, b \in G$ $\therefore$ $a\,b=b\,a$ as G is abelian.

Then $f(a)\,f(b)=f(a\,b)=f(b\,a)=f(b)\,f(a)$

$f(a), f(b) \in G'$ which therefore is abelian.

(5) *If f be a homomorphism of a group G* **into** *a group G' then prove that the homomorphic image $f(G)$ of G [It will not be G' as f is not onto] is a sub group of G'.*

Let $a, b \in G$ then $f(G)=\{f(a) : a \in G\}$.

Choose $a', b' \in f(G)$ so that $a'=f(a)$, $b'=f(b)$.

In order to prove $f(G)$ to be a sub group of G' we have to prove that

$$a', b' \in f(G) \Rightarrow a'\,b'^{-1} \in f(G)$$

Now $a'\,b'^{-1}=f(a)\,[f(b)]^{-1}=f(a)\,f(b^{-1})$

$$=f(a\,b^{-1}) \in f(G)$$
$$\because\quad a \in G, b \in G \Rightarrow a\,b^{-1} \in G$$

Thus $a', b' \in f(G) \Rightarrow a'\,b'^{-1} \in f(G)$ and hence $f(G)$ is a sub group.

§ 3. Kernel of homomorphism.

Definition. *If f is a homomorphism of a group G into a group G' then the set K of all those elements of G which are mapped onto the identity e' of G' is called the kernel of homomorphism of f.*

$$\therefore\quad K=\{x \in G : f(x)=e'\}.$$

Therom 1. *Prove that the kernel of a homomorphism $f : G \to G'$ is a normal sub gorup of G.*

(Meerut M. Sc. Summer 1969)

(Raj M. Sc. 66, 68)

$K=\{x \in G : f(x)=e'\}$.

Since $f(e)=e'$ $\therefore$ $e \in K$ *i.e.* **K is non empty.**

K is a sub group.

Let $a, b \in K \Rightarrow f(a)=e', f(b)=e'$

Now $f(a\ b^{-1})=f(a)\ f(b^{-1})=f(a)\ [f(b)]^{-1}$

$=e'\ (e')^{-1}=e'\ e'=e'$

Since $f(a\ b^{-1})=e' \Rightarrow a\ b^{-1} \in K$ whenever $a, b \in K$

Hence K is a sub group.

K is a normal sub group.

Let g be any element of G and $a \in K$ so that $f(a)=e'$.

If we show that $g\ a\ g^{-1} \in K$ then K will be a normal sub group.

Now $f(g\ a\ g^{-1})=f(g)\ f(a)\ f(g^{-1})=f(g)\ e'\ [f(g)]^{-1}$

$=f(g)\ [f(g)]^{-1}=e'$

$\therefore$ $g\ a\ g^{-1}$ also $\in K$. Hence K is normal sub group of G.

Theorem 2. *Let f be a homomorphism of a group G onto a group G' with kernel K and a be a given element of G such that $f(a)=a' \in G'$. Then the set of all those elements of G which have their image a' in G' in the coset Ka of K in G.*

In other words the set of all inverse image of a' under f is the right coset Ka, where a is any particular inverse image of a' in G.

$$K=\{x \in G : f(x)=e'\}.$$

Let us denote by A the set of all these elements of G which have the image a' in G'.

$\therefore$ $A=\{x \in G : f(x)=a'\}$.

We have to prove that $A=Ka$.

We shall establish that $A \subset Ka$ and $Ka \subset A$.

K a $\subset$ A. Let $y \in Ka \Rightarrow y=k\ a$

where $k \in K$ *i.e.* $f(k)=e'$

$\therefore$ $f(y)=f(k\ a)=f(k)\ f(a)=e'\ f(a)=f(a)=a'$.

Since $f(y)=a'$, it follows that $y \in A$.

$\therefore \quad y \in Ka \Rightarrow y \in A \quad \therefore \quad Ka \subset A$

A ⊂ K A. Let $z \in A \Rightarrow f(z)=a'$

Now $f(z\,a^{-1})=f(z)\,f(a^{-1})=f(z)\,[f(a)]^{-1}$

$=a'\,(a')^{-1} \quad \because \quad f(a)=a'$ given

$\therefore \quad f(z\,a^{-1})=e' \Rightarrow z\,a^{-1} \in K$ by def. of K.

$\Rightarrow (z\,a^{-1})\,a \in K\,a \Rightarrow z \in K\,a.$

$\therefore \quad z \in A \Rightarrow z \in K\,a, \quad \therefore \quad A \subset K\,a.$

Hence form (1) & (2) we prove that $A=K\,a$.

Theorem 3. *The necessary and sufficient condition for a homomorphism f of G onto G' with kernel K to be an isomorphism is that $K=\{e\}$.*

If f is to be an isomorphism then it is one-one and in that case $f(e)=e'$ where e and e' are the identities of G and G' respectively. No other element of G except e will have its image e' the identity of G'.

$\therefore \quad K=\{x \in G : f(x)=e'\}$ will consist of only one element e.

$\therefore \quad K=\{e\}$.

Conversely let $K=\{e\}$ be the kernel of homomorphism f of G onto G' so that $f(a)=a'$, $a \in G$, $a' \in G'$

Now f will be an isomorphism if f is one one

i.e. $f(b)=f(a) \Rightarrow b=a$.

Now if $f(b)=f(a)$ then $f(b)=a'$ so that b is also that element of G whose f-image is a' in G' and hence by preceeding theorem b should belong to right coset $K\,a$.

$\therefore \quad b \in K\,a, \quad \therefore \quad b=e\,a=a$ as $K=\{e\}$.

Hence $f(b)=f(a) \Rightarrow b=a$.

$\therefore$ f is one-one and hence an isomorphism.

Theorem 4. *Every quotient group G/H of a given group G is a homomorphic image of the group. Also prove that kernel of f is H* **(Delhi 69)**

Let G be a given group and H be any normal sub group of G so that G/H is a quotient group whose elements are of the type $H\,a, a \in G$.

We have to show that G/H is homomorphic image of G. For this we will show that a mapping f of G onto G/H such that $f(a\,b)=f(a)\,f(b) \quad \forall\ a, b \in G$

Consider the mapping $f: G \to G/H$ defined as

$$f(a)=H\,a,\ a \in G,\ H\,a \in G/H.$$

The mapping is onto. Corresponding to each element $H\,a$, $(a \in G)$ of $G/H\ \exists\ a \in G$ such that $f(a)=H\,a$.

Now if $a, b \in G$ then $f(a)=H\,a,\ f(b)=H\,b$.

$$f(a\,b)=H\,(a\,b)=(H\,a)\,(H\,b)=f(a)\,f(b).$$

Hence f is a homomorphism of G onto G/H.

Kernel of f. $f: G \to G/H$.

By definition kernel of f will be the sub set K of G whose f image is the identity of G/H which is H. **(P. 425)**

$\therefore \quad K=\{a \in G : f(a)=H\}$

We have to prove that K = H.

Let $a \in K \Rightarrow f(a)=H$ the identity of G/H.

By definition of f given above $f(a)=H\,a$

$$\therefore \quad H\,a=H \Rightarrow a \in H$$

$\therefore \quad a \in K \Rightarrow a \in H \quad \therefore \quad K \subseteq H$ ...(1)

Again let $h \in H$ then $H\,h=H$ by def. of cosets.

Now $f(h)=H\,h=H$ by def. of f

$$\therefore \quad h \in K$$

Hence $h \in H \Rightarrow h \in K \quad \therefore \quad H \subseteq K$ ...(2)

$\therefore$ form (1) and (2) we get **K = H.**

i.e. kernel of f is **H** where f is a homomorphism of G onto G/H.

Fundamental theorem on homomorphism of groups.

Theorem 5. *Every homomorphic image G' of a group G is isomorphic to some quotient group there of.*

(Meerut 69; Punjab 68; Delhi 69)

Let G be a group and G' be its homomorphic image under f.

If K be the kernel of f then as shown earlier K is normal sub group so that G/K is a quotient group.

We have to prove that G/K is isomorphic to homomorphic image G'.

i.e. $$\frac{G}{K} \cong G'$$

For proving this we will have to search out a one one onto mapping $\varphi : G/K \to G'$ which preserves the compositions.

If $a \in G$ then $Ka \in G/K$.

and $f(a) \in G'$ as $f : G \to G'$.

Hence in accordance with our definition.

$$\varphi(Ka) = f(a). \ \forall \ a \in G.$$

First of all we establish that the mapping is well defined *i.e.* independent of the particular element a chosen to represent the coset Ka of G/K.

i.e. if $Ka = Kb$ we will show that

$$\varphi(Ka) = \varphi(Kb)$$

Now $Ka = Kb \Rightarrow ab^{-1} \in K$

$\Rightarrow f(ab^{-1}) =$ Identity of G' as K is kernel of f

$\Rightarrow f(a) f(b^{-1}) = e'$ as f is homomorphism

$\Rightarrow f(a) [f(b)]^{-1} = e'$

$\Rightarrow f(a) [f(b)]^{-1} f(b) = e' f(b)$

$\Rightarrow f(a) e' = e' f(b)$

$\Rightarrow f(a) = f(b)$

$\Rightarrow \varphi(Ka) = \varphi(Kb)$

Hence the mapping is well defined.

For proving φ to be an isomorphism, it should be shown to be one-one onto and preserving the composition.

φ is one-one. $\varphi(Ka)=\varphi(Kb) \Rightarrow f(a)=f(b)$.

$\Rightarrow f(a)[f(b)]^{-1}=[f(b)][f(b)]^{-1}$

$\Rightarrow f(a)f(b)^{-1}=e'$ the identity of G'

$\Rightarrow f(a\,b^{-1})=e'$ as f is homomorphism

$\Rightarrow a\,b^{-1} \in K$

$\Rightarrow Ka=Kb$.

Hence φ is one-one.

φ is onto. Let any element of G' which is homomorphic image of G be $f(a)$, $a \in G$. Corresponding to this element $f(a)$ $\exists$ a coset Ka in G/K such that

$$\varphi(Ka)=f(a).$$

Hence φ is onto.

φ preserves the group compositions.

$\varphi[(Ka)(Kb)]=\varphi(Kab)=f(ab)$

$=f(a)f(b)$, as f is homomorphism

$=\varphi(Ka)\,\varphi(Kb)$

Hence φ is an isomorphism of G/K onto G'

i.e. $G/K \cong G'$.

Exercise 1

1. *If f is homomorphism of G onto G' and g is homomorphism of G' onto G''. Show that $g \circ f$ is a homomorphism of G onto G''. Prove also that the kernel of f is a sub group of the kernel of $g \circ f$.*

$f: G \cong G'$, $g: G' \cong G''$, both f and g are homomorphism (onto), and hence the composite mapping

$g \circ f: G \to G''$ is an onto mapping.

If it is to be homomorphism we should show that $g \circ f$ mapping preserves the composition of the groups.

Let $a, b \in G$ then

$(g \circ f)(ab)=g \circ [f(ab)]$ by def. of composite mapping

$=g[f(a)f(b)]$ $\because$ f is homomorphism

$$=g\,[\,f\,(a)\,]\,g\,[f\,(b)]$$
$$=(g\ o\ f)\ a.(g\ o\ f)\ b.$$

Hence $g\ o\ f$ preserves the composition and it therefore is a homomorphism of G onto G''.

Kernel of g o f.

If K be the kernel of $g\ o\ f$ then by definition,

$K=\{y \in G : (g\ o\ f)\ y=e''\}$ where e'' is identity of G''.

Let K' be the kernel of f, then

$K'=\{x \in G : f\,(x)=e'\}$ where e' is identity of G'

We have to prove that K' the kernel of f is a sub group of K the kernel of $g\ o\ f$.

Now both kernels K and K' are normal sub groups and hence in order to show that K' is a sub group of K it is sufficient to show that $K' \subseteq K$

Let $x \in K'$ then $f\,(x)=e'$.

Also $(g\ o\ f)\ x=g\,[f\,(x)]=g\,(e')=e''$

as g is a homomorphism of G' onto G'' and we know that the identities correspond.

Since $(g\ o\ f)\ x=e''$ where $g\ o\ f$ is homomorphism of G onto G'' it follows that x belongs to kernel K of $g\ o\ f$.

Hence $x \in K' \Rightarrow x \in K \quad \therefore \quad K' \subseteq K$.

Therefore the kernel of f is a sub group of the kernel of $g\ o\ f$.

2. *Prove that the mapping* $f : C \to R$ *such that* $f(x+iy)=x$ *is a homomorphism of the additive group of complex numbers onto the additive group of real numbers, find the kernel of* f.

Corresponding to any real number x $\exists$ a complex number $x+iy$ such that $f\,(x+iy)=x$ and as such f is an onto mapping. It will be a homomorphism if $\forall\ a, b \in C$

$f\,(a+b)=f\,(a)+f\,(b)$, groups are additive.

Let $a=x_1+iy_1$, $b=x_2+iy_2$
then $f(a)=x_1$. $f(b)=x_2$
Also $a+b=(x_1+x_2)+i(y_1+y_2)$
$\therefore$ $f(a+b)=x_1+x_2$ by def.
$=f(a)+f(b)$.
Hence f is a homomorphism (onto).

Kernel of f. It will consist of all those elements of C whose f image is the identity 0 of additive group of real numbers.

Since $f(x+iy)=x \Rightarrow f(0+iy)=0$ identity of R.

Hence kernel of f will be set of all those complex numbers whose real part is zero *i.e.* set of purely imaginary numbers.

3. *Prove that the mapping* $f: C \to C_0$ *such that* $f(z)=e^z$ *is a homomorphism of the additive group of complex numbers onto the multiplicative group of non zero complex numbers. What is the kernel of f.*

If $z_1, z_2 \in C$ then $f(z_1)=e^{z_1}, f(z_2)=e^{z_2}$.
f should preserve the compositions in the two groups. *i.e.* $f(z_1+z_2)$ should be shown to be $f(z_1)\,f(z_2)$.
as the composition in C is addition and that in C_0 is multiplication

$$f(z_1+z_2)=e^{z_1+z_2}=e^{z_1}\cdot e^{z_2}=f(z_1)\,f(z_2).$$

Hence f is a homomorphism.

Kernel of f. The identity of multiplicative group C_0 is 1 and we know that

$$f(2n\pi i)=e^{2n\pi i}=\cos\ n\pi+i\sin 2n\pi=1.$$

$\therefore$ Kernel of f=[$z \in C : f(z)$=identity of C_0]
$=\{2n\pi i\}$ where n is any integer.

4. *Let* C_0 *and* R_0 *be two multiplicative groups. Prove that the mapping* $f: C_0 \to R_0$ *such that* $f(z)=|z|$ *is a homomorphism. What is the kernel of f?* **(Raj. 1969)**

$f(z_1 z_2)=|z_1 z_2|=|z_1||z_2|=f(z_1) f(z_2)$

Hence f is homomorphism. The identity of R_0 is 1 and as such the kernel of f will consist of all those complex numbers whose module is 1 as $f(z)=|z|=1$ the identity of R_0.

5. *Let G be the multiplicative group of all $n\times n$ non singular matrices with elements as real numbers and let G' denote the multiplicative group of non zero numbers.*

Prove that the mapping

$f: G\to G'$ *such that* $f(A)=[A]$. $\forall\ A\in G$

is a homomorphism.

$f(A\ B)=|A\ B|=|A|\,|B|=f(A).f(B)$.

Hence f is homomorphism and the mapping is many one as more than one non-singular matrices may have their determinants whose value is same.

Endomorphism.

6. *Define* **endomorphism** *and prove that the mapping*

$f: C\to C$ *such that* $f(x+iy)=iy$

is an endomorphism of the additive group of complex numbers, What is the kernel of f ?

Definition A homomorphism of a group into itself is called an endomorphism.

$z_1=x_1+iy_1,\ z_2=x_2+iy_2$

$\therefore\ f(z_1)=iy_1,\ f(z_2)=iy_2$.

$z_1+z_2=(x_1+x_2)+i(y_1+y_2)$

$\therefore\ f(z_1+z_2)=i(y_1+y_2)=iy_1+iy_2=f(z_1)+f(z_2)$

Hence f preserves the group composition and is therefore endomorphism as it is mapping of a group into itself.

Identity of additive group C is zero hence all those numbers of the type $x+0i$ will be such whose f image will be $0i$ *i.e.* 0 *i.e.* the identity.

Therefore kernel of f will consist of all those complex numbers whose imaginary part is zero *i.e.* real numbers only.

7. *Prove that the mapping* $f : C_0 \to C_0$ *such that*

$$f(z)=z^n$$

where n is a +ive integer is an endomorphism of the multiplicative group of non zero complex numbers. What is the kernel of f. **(Raj. M.Sc. 1967)**

$f(z_1z_2)=(z_1z_2)^n=z_1^n z_2^n=f(z_1)\,f(z_2)$.

Hence an endomorphism.

The identity of multiplicative group C_0 is 1.

$f(z)=z^n$

$$\therefore \quad f\left(e^{\frac{2k\pi i}{n}}\right)=\left(e^{\frac{2k\pi i}{n}}\right)^n=e^{2k\pi i}$$

$$=\cos 2k\pi+i\sin 2k\pi=1.$$

$$\therefore \quad \text{kernel of } f=\left\{e^{\frac{2k\pi i}{n}}\right\} \text{ where } k \text{ is any integer}$$

§ 4. Automorphism of groups.

Definition. *An isomorphic mapping of a group G onto itself is called an automorphism of G.*

In other words $f : G \to G$ *such that*

f is one-one onto and

$$f(ab)=f(a)\,f(b),\ \forall\ a, b \in G$$

The composition in G being denoted multiplicatively is an automorphism of G.

Ex. 1. $f : I \to I$ *such that* $f(x)=-x\ \forall\ x \in I$.

Evidently the mapping is one-one onto.

Also $f(x_1+x_2)=-(x_1+x_2)=-x_1+(-x_2)$

$$=f(x_1)+f(x_2)$$

Hence f being an isomorphism of G onto itself is an automorphism of G.

Ex. 2. *The mapping $f : C \to C$ such that $f(z) = az$ where a is non zero complex nu ber is an automorphism of the additive group of complex numbers.*

Clearly the mapping is one-one because

$f(z_1) = f(z_2) \Rightarrow az_1 = az_2 \Rightarrow z_1 = z_2$.

The mapping is onto as for any complex number z

$\exists$ a complex number $\frac{z}{a}(a \neq 0)$

such that $f\left(\frac{z}{a}\right) = a \cdot \frac{z}{a} = z$.

Also $f(z_1 + z_2) = a(z_1 + z_2) = az_1 + az_2$

$= f(z_1) + f(z_2)$

Hence f being an isomorphism of C onto itself is an automorphism.

Group of automorphism of groups.

Theorem 6. *The set of all automorphism of a group forms a group with respect to composite of functions as the composition.* **(Punjab 68, Gujarat 70; Raj. M.Sc. 1966)**

Let $A(G) = \{f : f$ is an automorphism of $G\}$

such that f is one-one onto and preserves the group composition.

We have to show that $A(G)$ is a group w.r.t. composite of functions as the composition.

Axioms of a group.

1. Closure property. Let $f, g \in A(G)$, Since both are one-one onto therefore $g \circ f$ is also one-one-onto.

Again $(g \circ f)(ab) = go[f(ab)]$

$= go[f(a) f(b)]$ as f is automorphism

$= g[f(a)] g[f(b)]$

$= (g \circ f) a . (g \circ f) b$

Hence $g \circ f$ preserves the group composition which therefore is an automorphism and belongs to $A(G)$.

2. Associative. We know that composite of functions is associative and as such composite of automorphism is also associative.

3. Identity. The identity mapping I is one-one onto and preserves group composition and as such is an automorphism $\in A(G)$.

4. Inverse. If $f \in A(G)$ then f being one one onto the inverse mapping f^{-1} exists and is one-one onto. In order to show that f^{-1} is an automorphism we must show that it preserves group composition.

Let $f^{-1}(a)=a'$, $f^{-1}(b)=b'$

$\therefore \quad f(a')=a$, $f(b')=b$

Now $f^{-1}(ab)=f^{-1}[f(a')\,f(b')]$

$=f^{-1}[f(a'b']$ $\because$ f is automorphism

$=a'b'=f^{-1}(a)\,f^{-1}(b)$.

Hence f^{-1} preserves group composition and is therefore an automorphism $\in A(G)$.

Thus all the axioms of a group are satisfied and we can say that the set of all automorphism of a group is a group under composite composition.

Ex. 3. *If a is any given non zero complex number, show that* $f_a : C \to C$ *such that* $f_a(z)=az$ *is an automorphism of the additive group of complex numbers.*

Prove also that the totality of these automorphisms arising from all non zero complex numbers a is an abelian group for the composite composition. Show also that the group is isomorphic to the multiplicative group C_0 *of all non-zero complex numbers.*

Ist part f_a is an automorphism we have proved in Ex. 2. P. 443.

2nd part. Let $A=\{f_a : a \neq 0$ and f_a is an automorphism$\}$

We have to show that the set A is an abelian group for composite compositions.

Axioms of a group.

Closure property. Let $f_a, f_b \in A$ then

$$f_a \, o \, f_b \, (z) = f_a \, [f_b \, (z)] = f_a \, (bz) = a \, (bz)$$
$$= ab \, (z) = f_{ab} \, (z).$$

$\therefore \quad f_a \, o \, f_b = f_{ab}$, where $ab \neq 0$ as $a \neq 0$. $b \neq 0$

$\therefore \quad f_{ab} \in A$, and hence $f_a \, o \, f_b \in A$.

Thus closure property is satisfied.

Associative. $(f_a \, o \, f_b) \, o \, f_c = (f_{ab}) \, o \, f_c = f_{(ab)c}$
$= f_{a(bc)} = f_a \, f_{bc}$
$= f_a \, o \, [f_b \, o \, f_c] \quad \because \; (ab)c = a \, (bc)$

Hence associative.

Identity. We know that 1 is the identity of a group of non zero complex numbers C_0 for multiplicative composition so that $1 . a = a = a . 1$

Now $f_1 \, o \, f_a = f_{1a} = f_a, \; \forall \; f_a \in A$.

Hence $f_1 \in A$ is the identity of A.

Inverse. We know that $a \neq 0$, $a \, a^{-1} = a^{-1} a = 1$

Now $f_a \, o \, f_a^{-1} = f_{a \, a^{-1}} = f_1 =$ Identity of A.

Hence f_a^{-1} where $a^{-1} \neq 0$ is the inverse of f_a and clearly $f_a^{-1} \in A$.

Abelian. Since multiplication of complex numbers is commutative we have $ab = ba$.

$\therefore \quad f_a \, o \, f_b = f_{ab} = f_{ba} = f_b \, o \, f_a$

Thus the set A of all automorphisms of C defined as given constitutes an abelian group w. r. t. composite compositions.

3rd Part. We have to prove that group A of automorphism is isomorphic to group $(C_0, \times)$ *i e.* $A \cong (C_0, \times)$. or $(C_0, \times) \cong A$ as the relation of isomorphism being an equivalence relation is symmetric.

In order to prove $C_0 \cong A$ we have to search out a one-one onto mapping preserving the compositions.

Let us define $\varphi : C_0 \to A$ such that $\varphi(a) = f_a$, $a \neq 0$

The mapping φ is one one.

$\varphi(a) = \varphi(b) \Rightarrow f_a = f_b \Rightarrow f_a(z) = f_b(z)$

$\Rightarrow az = bz \Rightarrow a = b$ by Cancelation law

The mapping is clearly onto.

Let us verify about **composition preservation.**

$\varphi(ab) = f_{ab} = f_a \, o \, f_b = \varphi(a) \, o \, \varphi(b)$.

Thus the mapping preserves the compositions in the groups.

Hence φ is an isomorphism of C_0 onto A.

or $C_0 \cong A$ or $B \cong C_0$.

§ 5. **Inner Automorphism.**

Theorem 7. *Corresponding to a fixed element a of a group G prove that the mapping $f_a : G \to G$ such that $f_a(x) = a^{-1} x a$ is an automorphism of G.*

(Aligarh 65; Delhi 64)

$f_a(x) = f_a(y) \Rightarrow a^{-1} xa = a^{-1} ya \Rightarrow x = y$ by Cancelation Law. Hence f_a is **one-one.**

Let y be any element then $ay\,a^{-1}$ is also an element of G and $f_a(ay\,a^{-1}) = a^{-1}(ay\,a^{-1})\,a = (a^{-1}\,a)\,y\,(a^{-1}\,a) = y$.

Thus corresponding to each y in G $\exists$ $x = ay\,a^{-1}$ in G such that $f_a(x) = y$. Hence f_a is onto.

Again $f_a(xy) = a^{-1}(xy)\,a = a^{-1} x (a\,a^{-1}) ya.$

$= (a^{-1} xa)\,(a^{-1} ya) = f_a(x).f_a(y)$

Thus f_a preserves the group composition.

Hence f_a is an automorphism.

Inner automorphism.

The mapping $f_a : G \to G$ such that

$f_a(x) = a^{-1} xa \;\forall\; x \in G$

which is an automorphism of G is called

Inner autumorphism and an automorphism which is not an inner automorphism is called outer automorphism.

Nature of Inner automorphism for abelian and non abelian groups. **(Raj. M. Sc. 66)**

Let f_a be an inner automorphism on a group G

$f_a(x) = a^{-1} xa$ by def. $\forall\ x \in G$

$= a^{-1}(ax)$ if G is abelian *i.e.* $xa = ax$

$= (a^{-1} a)\, x = ex = x = I(x)$

$\therefore\ f_a = I$ *i.e.* identity mapping.

Hence for abelian groups the only inner automorphism is the identity mapping But if G is non abelian then

$f_a(x) = a^{-1} x a \neq x \neq I(x)$

i.e. $f_a \neq I$

Thus for non abelian group $\exists$ non trivial ($\neq I$) inner automorphism.

Theorem 8. Group of Inner automorphism.

The set of all inner automorphisms of a group G is normal sub group of the group of its automorphisms, isomorphic to the quotient group G/Z where Z is the centre of G.

(Aligarh 65; Delhi 70; Meerut M. Sc. 1967)

We have shown that the set of automorphisms is a group to be denoted by $A(G)$.

$\therefore\ A(G) = \{ f : f : G \to G$ and f is an isomorphism$\}$

Now inner automorphism are also automorphisms as such they also form a group to be defined by $I(G)$.

$\therefore\ I(G) = \{ f_a : f_a : G \to G$ such that $f_a(x) = a^{-1} xa\}$

where f_a is also an automorphism called inner automorphism.

Ist step. We have to prove that $I(G)$ is a sub group of $A(G)$.

It is evident that $I(G) \subseteq A(G)$ and if it is to be sub group we should show that $[a \in H, b \in H \Rightarrow ab^{-1} \in H$ for H to be a sub group $G]$.

$f_a \in I(G), f_b \in I(G) \Rightarrow f_a [f_b]^{-1} \in I(G)$

Let us first define $[f_b]^{-1}$

$[f_b f_b^{-1}] x = f_b [f_b^{-1} x] = f_b [(b^{-1})^{-1} x b^{-1}]$ by def. of f_a

$= f_b [bx\ b^{-1}] = b^{-1} [bx\ b^{-1}] b$

$= b^{-1} bx\ b^{-1} b = ex\ e = x = Ix$

$\therefore \quad f_b f_b^{-1} =$ Identity mapping on G

$\therefore \quad [f_b]^{-1} = f_b^{-1}$ .. (1)

Now $f_a [f_b]^{-1} x = f_a f_b^{-1} x) = f_a [f_b^{-1} x]$

$= f_a [(b^{-1})^{-1} x\ b^{-1}] = f_a [b\ x\ b^{-1}]$

$= a^{-1} bx\ b^{-1} a = (b^{-1} a)^{-1} x\ (b^{-1} a)$

$= f_b^{-1} a\ (x)$ by def. of f_a.

But $b^{-1} a \in G \Rightarrow f_b^{-1} a \in I(G)$

$\therefore \quad f_a [f_b]^{-1} = f_b^{-1} a \in I(G)$

Then $f_a, f_b \in I(G) \Rightarrow f_a [f_b]^{-1} \in I(G)$ which is a sub set of $A(G)$

Hence $I(G)$ is a sub groud $A(G)$.

2nd Step. To show that I (G) is a normal sub group of A (G).

Criteria for normal sub group A sub group H of G will be normal if $x\ h\ x^{-1} \in H\ \forall\ h \in H$ and $\forall\ x \in G$.

Let f be any element of $A(G)$ and f_a be any element of $I(G)$.

In order to show that sub group $I(G)$ of $A(G)$ is a normal sub group we should establish that $f f_a f^{-1} \in I(G)$.

Now $[f f_a f^{-1}](x) = f f_a [f^{-1}(x)]$

$= f [a^{-1} f^{-1}(x)\ a]$ by def of f_a.

$= f(a^{-1}) f f^{-1}(x)\ f(a)$.

$\because$ f being an automorphism is composition preserving

$= [f(a)]^{-1} x f(a)$ $\because$ $f(a^{-1}) = [f(a)]^{-1}$ and $f f^{-1} x = I x = I x = x$

$= c^{-1}\ x\ c$ where $c = f(a) \in G$

$= f_c\ x$ where $f_c \in I(G)$.

Hence $f\, f_a\, f^{-1} = f_c \in I(G)\ \forall\ f \in A(G)$ and $f_a \in I(G)$.

Therefore $I(G)$ is a normal sub group of $A(G)$.

3rd Step. To show that I (G) is isomorphic to G/Z.

$I(G) \cong G/Z$ or $G/Z \cong I(G)$.

Method. From Fundamental Theorem of Homomorphism.

We know that every homomorphic image G' of a group G is isomorphic to some quotient group thereof.

So we shall first prove that $I(G)$ is homomorphic image of group G and Z is the kernel of this homomorphism which we know is a normal sub group so that G/Z is a quotient group.

After proving this we can at once say that $G/Z \cong I(G)$.

To prove that $I(G)$ is homomorphic image of G.

Let us define a mapping $\varphi : G \to I(G)$.

such that $\varphi(a) = f_{a^{-1}}\ \forall\ a \in G$.

The mapping φ is onto because if f_x be an element of $I(G)$ then $\exists\ x^{-1}$ in G such that $\varphi(x^{-1}) = f_{(x^{-1})^{-1}} = f_x$.

Hence φ is onto.

φ Preserves compositions.

$$\left.\begin{array}{l}\varphi(a) = f_{a^{-1}},\ \varphi(b) = f_{b^{-1}} \\ \text{Also } \varphi(a\,b) = f_{(ab)^{-1}}\end{array}\right\} \ldots(A)$$

$$\therefore\ f_{(ab)^{-1}}(x) = [(ab)^{-1}]^{-1}\ x\ (ab)^{-1}$$

$$= ab\ x\ b^{-1}\ a^{-1}$$

$$= (a^{-1})^{-1}\ (bx\ b^{-1})\ a^{-1}$$

$$= f_{a^{-1}}(bx\ b^{-1})$$

$$= f_{a^{-1}}[(b^{-1})^{-1}\ x\ b^{-1}]$$

$$= f_{a^{-1}}[f_{b^{-1}} x] = (f_{a^{-1}} f_{b^{-1}})\ x$$

$\therefore \quad f_{(ab)^{-1}}=f_{a^{-1}}f_{b^{-1}}$

$\therefore \quad \varphi\,(ab)=\varphi\,(a)\,\varphi\,(b)$ by A.

Hence the mapping φ is homomorphism of G onto $I\,(G)$ and as such $I\,(G)$ is homomorphic image.

4th Step. Kernel of homomorphism $\phi : G \to I\,(G)$, is the set of all those elements of G whose φ image is the identity of $I\,(G)$ *i.e.* I.

If Z be the kernel of φ then

$$Z=\{z : \varphi\,(z)=I\}.$$

But $\varphi\,(z)=f_{z^{-1}}$ or $I=f_{z^{-1}}$

or $f_{z^{-1}}(x)=Ix \quad \forall \quad x \in G.$

or $(z^{-1})^{-1}\,x\,z^{-1}=x.$

or $zxz^{-1}=x$ or $zx=xz \ \forall \ x \in G$ and $z \in Z$.

i.e. Z is the centre of G.

Hence kernel of ϕ is the centre Z of G which we know is a normal sub group. Therefore G/Z is a quotient group.

Now from fundamental theorem of homomorphisms.

$G/Z \cong I\,(G)$ where $I\,(G)$ is homomorphic image of group G under homomorphism φ as shown above whose kernel is shown to be Z.

Hence the theorem.

§ 6. External direct products.

Definition. *If G_1 and G_2 be two groups then the set of all ordered pairs $(g_1, g_2) : g_1 \in G_1, g_2 \in G_2$, is called the external direct product of G_1 by G_2. The external direct product of G_1, by G_2 is expressed as $G_1 \times G_2$.*

Note. It should be clearly understood that

$$G_1 \times G_2 \neq G_2 \times G_1.$$

Also $G_1 \times G_2$ is not same as G_1G_2, because

$G_1G_2=\{g_1g_2 : g_1 \in G_1, g_2 \in G_2\}$. where as

$G_1 \times G_2=\{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$

1.Theorem 9. *If G_1, G_2 be any two abstract groups then the set*

$$G_1 \times G_2 = \{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$$

is a group with respect to the binary operation denoted multiplicatively and defined as

$$(g_1, g_2)\ (h_1, h_2) = (g_1\ h_1, g_2\ h_2) \qquad \ldots(1)$$

where g , $h_1 \in G_1$, g_2, $h_2 \in G_2$.

Proof. **Axioms of a group**

1. Closure property.

$g_1, h_1 \in G_1 \Rightarrow g_1h_1 \in G_1$ as G_1 is a group

$g_2, h_2 \in G_2 \Rightarrow g_2h_2 \in G_2$ as G_2 is a group.

$\therefore \quad (g_1h_1, g_2h_2) \in G_1 \times G_2$.

2. Associative.

$$[(g_1, g_2)\ (h_1, h_2)]\ (k_1, k_2)$$
$$= (g_1h_1, g_2h_2)\ (k_1, k_2)$$
$$= [(g_1h_1)\ k_1, (g_2h_2)\ k_2]$$
$$= [g_1\ (h_1k_1), g_2\ (h_2k_2)] \quad \because \quad G_1, G_2 \text{ are groups.}$$
$$= (g_1, g_2)\ [(h_1k_1, h_2k_2)]$$
$$= (g_1, g_2)\ [\ h_1, h_2)\ (k_1, k_2)].$$

Hence the composition is associative.

3. Existence of identity.

If e_1, e_2 be the identities of groups G_1 and G_2 respectively then

$$(e_1, e_2) \in G_1 \times G_2.$$

Also $g_1e_1 = e_1g_1 = g_1$

and $g_2e_2 = e_2g_2 = g_2$.

Now $(g_1, g_2)\ (e_1, e_2) = (g_1e_1, g_2e_2) = (g_1, g_2)$

and $(e_1, e_2)\ (g_1, g_2) = (e_1g_1, e_2g_2) = (g_1, g_2)$.

Hence $(e_1, e_2) \in G_1 \times G_2$ is the identity element of $G_1 \times G_2$.

4. Existence of Inverse.

$g_1 \in G_1 \Rightarrow g_1^{-1} \in G_1$, $g_2 \in G_2 \Rightarrow g_2^{-1} \in G_2$.

and $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$.

Also $g_1 g_1^{-1} = g_1^{-1} g_1 = e_1$, $g_2 g_2^{-1} = g_2^{-1} g_2 = e_2$. ...(A)

Since $(g_1, g_2)\ (g_1^{-1}, g_2^{-1}) = (g_1^{-1}, g_2^{-1})\ (g_1, g_2)$

$= (e_1, e_2)$ the identity by relations in (A)

it follows that $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$.

Thus the inverse exists and belongs to the set.

Hence $G_1 \times G_2$ is a group with respect to the binary composition defined before,

Theorem 10. *If G_1, G_2 are groups then the sub sets $G_1 \times \{e_2\}$ and $\{e_1\} \times G_2$ of $G_1 \times G_2$ are normal sub groups of $G_1 \times G_2$ isomorphic to G_1 and G_2 respectively,*

$G_1 \times \{e_2\}$ is a sub group of $G_1 \times G_2$

H will be a sub group if $a \in H$, $b \in H \Rightarrow ab^{-1} \in H$.

Choose $a = (g_1, e_2)$, $b = (h_1, e_2) \in G_1 \times \{e_2\}$

then $ab^{-1} = (g_1, e_2)\ (h_1, e_2)^{-1} = (g_1, e_2)\ (h_1^{-1}, e_2^{-1})$

$= (g_1, e_2)\ (h_1^{-1}, e_2) = (g_1 h_1^{-1}, e_2 e_2)$

$= (g_1 h_1^{-1}, e_2) \in G_1 \times \{e_2\}$

$\because$ $g_1 \in G_1, h_1 \in G_1 \Rightarrow h_1^{-1} \in G_1$ hence $g_1 h_1^{-1} \in G_1$.

Above relation shows that $G_1 \times \{e_2\}$ is a sub group of $G_1 \times G_2$.

Similarly we can show that $\{e_1\} \times G_2$ is a sub group of $G_1 \times G_2$.

$G_1 \times \{e_2\}$ is a normal sub group of $G_1 \times G_2$

A sub group H of G will be a normal sub group of G if for $h \in H$, $x\ h\ x^{-1} \in H\ \forall\ x \in G$.

Here $H = G_1 \times \{e_2\}$ so that $h \in H$ is (g_1, e_2)

$G = G_1 \times G_2$ so that $x \in G_1 \times G_2$ is (p, q),

$p \in G_1, q \in G_2$.

Now $x\ h\ x^{-1} = (p, q)\ (g_1, e_2)\ (p, q)^{-1}$

$= (p, q)\ (g_1, e_2)\ (p^{-1}, q^{-1})$

$= (p g_1 p^{-1}, q e_2 q^{-1})$

$= (p g_1 p^{-1}, e_2) \in G_1 \times \{e_2\}$

because $p, g_1, p^{-1} \in G_1 \Rightarrow p g_1 p^{-1} \in G_1$ and $q\ e_2\ q^{-1} = e_2$.

Hence $G_1 \times \{e_2\}$ is a normal sub group of $G_1 \times G_2$.

Similarly $e_1 \times \{G_2\}$ is a normal sub group of $G_1 \times G_2$.

$G_1 \times \{e_2\}$ is isomorphic to G_1

Let $f : G_1 \times \{e_2\} \to G_1$ defined as

$$f[(g_1, e_2)] = g_1$$

clearly f is one-one as $f[(g_1, e_2)] = f[(h_1, e_2)] \Rightarrow g_1 = h_1$

$$\Rightarrow (g_1, e_2) = (h_1, e_2)$$

Also f is onto.

Again $f[(g_1, e_2)\ (h_1, e_2)] = f(g_1 h_1, e_2)] = g_1 h_1.$

$$= f(g_1, e_2)\, f(h_1, e_2)$$

i.e. $f(ab) = f(a)\, f(b) \quad \forall \quad a, b \in G_1 \times \{e_2\}.$

Hence $G_1 \times \{e_2\} \cong G_1$

In a similar manner we can prove that $\{e_1\} \times G_2 \cong G_2$

Theorem 11. *If G_1 and G_2 are groups then prove the following.*

(*a*) $G_1 \times \{e_2\} \cap \{e_1\} \times G_2 = (e_1, e_2)$.

Let $x \in A \cap B \Rightarrow x \in A$ and $x \in B$.

$\therefore\ x \in G_1 \times \{e_2\} \Rightarrow x = (g_1, e_2)$.

This x can belong to $\{e_1\} \times G_2$ if $g_1 = e_1$

because in that case

$x = (e_1, e_2) \in \{e_1\} \times G_2$.

Hence (e_1, e_2) which is identity of group $G_1 \times G_2$ is the only element common to $G_1 \times \{e_2\} \cap \{e_1\} \times G_2$

(*b*) *Every element of $G_1 \times \{e_2\}$ commutes with every* element of $\{e_1\} \times G_2$.

Let $a \in G_1 \times \{e_2\} = (g_1, e_2),\ g_1 \in G_1$

$b \in \{e_1\} \times G_2 = (e_1, g_2),\ g_2 \in G_2$.

$a\, b = (g_1, e_2)\ (e_1, g_2) = (g_1 e_1, e_2 g_2) = (g_1, g_2)$

$b\, a = (e_1, g_2)\ (g_1, e_2) = (e_1 g_1, g_2 e_2) = (g_1, g_2)$.

$\therefore\ ab = ba.$

Hence every element of $G_1 \times \{e_2\}$ commutes with every element of $\{e_1\} \times G_2$.

(*c*) *Every element of $G_1 \times G_2$ can be uniquely expressed as the product of an element of $G_1 \times \{e_2\}$ by an element of* $\{e_1\} \times G_2$.

Let any element of $G_1 \times G_2$ be (g_1, g_2) then

$(g_1, g_2) = (g_1 e_1, e_2 g_2) = (g_1, e_2)\ (e_1, g_2)$

$=$ Product of an element of $G_1 \times \{e_2\}$ by an element of $\{e_1\} \times G_2$.

Above relation shows that there is at least one representation.

Now if $(g_1, g_2) = (h_1, e_2)\ (e_1, h_2)$ be another representation as above

then $(g_1, g_2) = (h_1 e_1, e_2 h_2) = (h_1, h_2)$

$\Rightarrow g_1 = h_1,\ g_2 = h_2$.

Hence the representation is unique.

(*d*) $G_1 \times G_2 \cong G_2 \times G_1$.

Let $f : G_1 \times G_2 \to G_2 \times G_1$ defined as

$$f\ (g_1, g_2) = (g_2, g_1)$$

clearly the mapping is one-one-onto.

Also $f\ [(g_1, g_2)\ (h_1, h_2)] = f\ (g_1 h_1, g_2 h_2) = (g_2 h_2, g_1 h_1)$

$= (g_2, g_1)\ (h_2, h_1)$

$= [f\ (g_1, g_2)]\ [f\ (h_1, h_2)]$

$\therefore \quad G_1 \times G_2 \cong G_2 \times G_1$.

CHAPTER VII

QUOTIENTS RING AND RING HOMOMORPHISM

§ 1. Quotient Ring.

Theorem 1. *Let R be a ring and S be a two sided ideal of R. Prove that the set $\overline{R}$ or R/S of all distinct cosets $S+a$, $(a \in R)$ of S in R which are obtained by considering S as a sub group of R under addition is a ring under the two composition in $\overline{R}$ defined as*

$$(S+a)+(S+b)=S+(a+b)$$
$$(S+a).(S+b)=S+ab.$$

(Meerut M.Sc. 68; Raj. M.Sc. 66)

First of all we shall establish that the above two compositions are well defined *i.e.* they are not dependent on some particular elements like a and b chosen for the cosets :

For this we will establish that if

$$S+a=S+a' \quad \text{and} \quad S+b=S+b' \text{ then}$$
$$(S+a)+(S+b)=(S+a')+(S+b')$$

and
$$(S+a)\ (S+b)=(S+a')\ (S+b').$$

The following points studied in sub group be noted

$$Ha=Hb \Rightarrow ab^{-1} \in H$$
$$H+a=H+b \Rightarrow a-b \in H. \qquad \ldots (1)$$

Also $Hh=H$ if $h \in H$

or $H+h=H$ if $h \in H$. $\qquad \ldots (2)$

Proof. $S+a=S+a' \Rightarrow S=S+a'-a$

$\Rightarrow a'-a \in S$ by (2) $\Rightarrow a'=a+\alpha,\ \alpha \in S.$

Similarly $S+b=S+b' \Rightarrow b'=b+\beta,\ \beta \in S.$

$\therefore \quad a'+b'=(a+\alpha)+(b+\beta)=(a+b)+(\alpha+\beta)$

or $\quad (a'+b')-(a+b)=\alpha+\beta \in S$

$\Rightarrow S+(a'+b')=S+(a+b)$ by (1)

$\Rightarrow (S+a')+(S+b')=(S+a)+(S+b)$ by def.

Again $a'b'=(a+\alpha)\,(b+\beta)=ab+\alpha b+a\beta+\alpha\beta.$

$\therefore \quad a'b'-ab=\alpha b+a\beta+\alpha\beta.$

Now $\alpha \in S, b \in R \Rightarrow \alpha b \in S$ as S is an ideal

$a \in R, \beta \in S \Rightarrow a\beta \in S$ as S is an ideal

$\alpha \in S, \beta \in S \Rightarrow \alpha\beta \in S.$

$\therefore \quad a'b'-ab \in S$

$\therefore \quad S+a'b'=S+ab$ by (1)

$\Rightarrow (S+a')\,(S+b')=(S+a)\,(S+b).$

Hence the two compositions are well defined.

Now we shall prove that $\bar{R}$ is a ring.

R_1. **$\bar{R}$ is an additive abelian group.**

1. $(S+a)+(S+b)=S+(a+b)$,

where $a+b \in R$ as R is a ring.

$\therefore \quad S+(a+b) \in \bar{R}.$

2. **Addition is associative.**

$(S+a)+[(S+b)+(S+c)]=(S+a)+[S+(b+c)]$

$=S+a+(b+c)=S+(a+b)+c$

because addition in R is associative.

$=[S+(a+b)]+(S+c)$

$=[(S+a)+(S+b)]+(S+c).$

3. **Identity.** $S=S+0 \in \bar{R}.$

Also $(S+0)+(S+a)=S+(0+a)=S+a.$

$\therefore$ S is the additive identity.

4. **Additive inverse.**

$(S+a)+[S+(-a)]=S+[a+(-a)]=S+0=S.$

Hence $S+(-a)$ is additive inverse of $S+a \in \bar{R}$.

5. Addition is Commutative.

$$(S+a)+(S+b)=S+(a+b)=S+(b+a)$$
$$=(S+b)+(S+a)$$

because addition is commutative in R.

Hence $\bar{R}$ is an additive abelian group.

R_2. Multiplication is a binary composition which is associative

$$a, b \in R \Rightarrow ab \in R.$$

$\therefore \quad (S+a).(S+b)=S+ab \in \bar{R}$ as $ab \in R$.

Also $\quad (S+a)\,[(S+b)\ (S+c)]=(S+a)\ (S+bc)$
$$=S+a\,(bc)=S+(ab)c$$
$$\because \quad a(bc)=(ab)c \text{ in } R.$$
$$=(S+ab)(S+c)=[(S+a)(S+b)](S+c).$$

R_3. Multiplication distributes addition

$$(S+a)\,[(S+b)+(S+c)]=(S+a)\ (S+b+c)$$
$$=S+a\,(b+c)=S+ab+ac.$$
$$\because \quad a\,(b+c)=ab+ac \text{ in } R$$
$$=(S+ab)+(S+ac)$$
$$=(S+a)\ (S+b)+(S+a)\ (S+c).$$

Similarly we can prove the other distributive law.

Hence $\bar{R}$ is a ring with respect to the given compositions the zero of the ring being $S+\mathbf{0}$ *i e.* S.

Alternative notation. The ring $\bar{R}$ is also denoted as R/S is called quotient ring or **ring of residue classes.**

(Raj. M.Sc. 67, 69)

Note. If R is commutative then $\bar{R}$ or R/S is also commutative given $ab=ba$ as R is commutative.

$\therefore \quad (S+a)\ (S+b)=S+ab=S+ba=(S+b)\ (S+a)$.

Hence R/S is also commutative

If R is a ring with unity 1 then $\bar{R}$ or R/S is also a ring with unity, the unity being S+1.

Since R is with unity $\therefore \quad a.1=a.$

$\therefore \quad (S+a)\,(S+1)=(S+a.1)=S+a.$

$\therefore \quad (S+1)$ is unity of ring $\bar{R}$ or R/S.

Ex. 1. *Let $(I_0, +, .)$ be the ring of integers and let $S=\ldots, -15, -10, -5, 0, 5, 10, 15, \ldots$ be an ideal of the ring. Prove that I/S is a ring and show further that it is a field.*

Now $I=\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
the element of I/S will be cosets $S+a : a \in I$

we shall have only the following five distinct cosets
i.e. $S, S+1, S+2, S+3$ and $S+4$.

It is easy to observe that the coset $S+5$ will be same as coset S, coset $S+6$ was to the same as coset $S+1$ etc.

$\therefore \quad I/S=\{S, S+1, S+2, S+3, S+4\}$
with the definition of addition and multiplication as

$$(S+a)+(S+b)=S+(a+b) \qquad \ldots (1)$$

$$(S+a)\,(S+b)=S+ab) \qquad \ldots (2)$$

we have the following composition tables for I/S both for addition and multiplication.

+	S	$S+1$	$S+2$	$S+3$	$S+4$
S	S	$S+1$	$S+2$	$S+3$	$S+4$
$S+1$	$S+1$	$S+2$	$S+3$	$S+4$	S
$S+2$	$S+2$	$S+3$	$S+4$	S	$S+1$
$S+3$	$S+3$	$S+4$	S	$S+1$	$S+2$
$S+4$	$S+4$	S	$S+1$	$S+2$	$S+3$

·	S	$S+1$	$S+2$	$S+3$	$S+4$
S	S	S	S	S	S
$S+1$	S	$S+1$	$S+2$	$S+3$	$S+4$
$S+2$	S	$S+2$	$S+4$	$S+1$	$S+3$
$S+3$	S	$S+3$	$S+1$	$S+4$	$S+2$
$S+4$	S	$S+4$	$S+3$	$S+2$	$S+1$

It is easy to establish from first table that the set I/S is an additive abelian group, S being a zero element.

From the second table we can prove that multiplication is a binary composition which is associative. Also it distributes addition. Hence I/S is a ring.

Again from the 2nd table we find that multiplication is commutative and also $S+1$ is the unity of the ring. The non zero element of the ring are $S+1$, $S+2$, $S+3$, $S+4$ whose inverses from 2nd table are $S+1$, $S+3$, $S+2$, $S+4$ respectively. Thus ring I/S is a commutative ring, with unity in which every non-zero element is inversible and hence it is a field.

Theorem 2. *An ideal S of a commutative ring R with unity is maximal if and only if the quotient ring R/S is a field.*

As shown in note on page 457 the quotient ring R/S will also be a commutative ring with unity as R is like that.

$S+1$ is the unity of the quotient ring where 1 is the unity of the ring R and S is the zero (additive identity)

1st case. given : S is a maximal ideal

To prove that R/S is a field.

In order to show R/S to be a field we have already shown it to be a commutative ring with unity and we have only to show that all non-zero elements of R/S are inversible.

Let $S+b$ be a non-zero element of R/S *i.e.* $S+b \neq S$ *i.e.* $b \notin S$. Now if (b) is the principal ideal of R then $S+(b)$ is also an ideal of R.

Also $b \notin S$

$$\therefore \quad S \subseteq S+(b)$$

But S is given to be maximal ideal of R and hence by definition we must have $S+(b)=R$

$\therefore \quad a+\alpha b=1$ where $a \in S$, $\alpha\, b \in (b)$, $\alpha \in R$

and $1=$unity of R or $1-\alpha b=a \in S$

$\therefore \quad S+1=S+\alpha b=(S+\alpha)(S+b)$

But $S+1$ is unity of R/S and hence $(S+b)^{-1}=S+\alpha$

Thus $S+b$ is inversible and hence R/S is a field.

Converse. Given R/S is a field and S is an ideal of R.

To prove S is a maximal ideal

Let S' be any other ideal properly containing S *i.e.* $S \subseteq S' \subseteq R$. By definition S will be a maximal ideal. If we establish that $S'=R$. But $S' \subseteq R$ as S' is an ideal and hence we have only to establish that $R \subseteq S'$.

Now as $S \subseteq S'$ therefore all those elements of R contained in S belong to S', hence $R \subseteq S'$ if all these elements α of $R \notin S$, also belong to S'.

Let $\alpha \in R$, $\alpha \notin S$ then $S+\alpha \neq S$ *i.e.* zero of R/S.

Thus $S+\alpha$ is a non-zero element of R/S. Also $S \subseteq S'$ and hence there exists β in S' which is not contained in S.

Therefore $S+\beta \neq S$ (as $\beta \notin S$) is also a non-zero element of R/S.

Also R/S is given to be a field and in a field non-zero elements form a multiplicative group (see page 195). Therefore there exists another non-zero element $S+x$ of R/S such that

$$(S+x)\,(S+\beta)=S+\alpha \quad \alpha, x \in R, \beta \in S'$$
$$\Rightarrow S+x\beta=S+\alpha$$

$\Rightarrow x\beta-\alpha \in S$

$\Rightarrow x\beta-\alpha \in S'$ as $S \subseteq S'$

But S' is an ideal $\therefore$ $x \in R, \beta \in S' \Rightarrow x\beta \in S'$

Now $x\beta \in S'$, $x\beta-\alpha \in S' \Rightarrow x\beta-(x\beta-\alpha) \in S'$

$\Rightarrow \alpha \in S'$

$\therefore$ $\alpha \in R \Rightarrow \alpha \in S'$

$\therefore$ $R \subseteq S'$ also $S' \subseteq R$

$\therefore$ $S'=R$

Hence S' is maximal ideal.

§ 2. Ring Homomorphism.

Definitions.

(a) Homomorphism onto :

A mapping f from a ring R onto a ring R' is called homomorphism of R onto R' if $\forall$ $a, b \in R$

$$f(a+b)=f(a)+f(b) \quad \ldots(1)$$

$$f(a.b)=f(a).f(b). \quad \ldots(2)$$

In this case the ring R' is said to be **homomorphic image** of ring R, or else, the ring is said to homomorphic to ring R'. Symbolically we say $R \simeq R'$. It may be noted that for isomorphism we use the symbol $\cong$ *i.e.* $R \cong R'$ and for homomorphism the symbol is $\simeq$.

On the left hand side the $+,.$ denote the two compositions in R whereas on the right they denote the compositions in R'.

Distinction between isomorphism and homomorphism (onto)

The isomorphic mapping shou'd be necessarily **one-one** and onto satisfying the above results 1 and 2 whereas a homomorphic (onto) mapping need not be necessarily one-one It may be many one.

Again we know that the relation of isomorphism in the set of rings is an equivalence relation but the relation of homomorphism will not be an equivalence relation for in this case the relation of homomorphism will not be symmetric as we know that only one-one-onto mapping are inversible and in this case the mapping is not necessarily one-one In other words $R \simeq R'$ does not imply $R' \simeq R$ whereas

$$R \cong R' \Rightarrow R' \cong R.$$

(b) Homomorphism into.

A mapping f from a ring R into a ring R' is called homomorphism of R into R' if $\forall\ a, b \in R$

$$f(a+b)=f(a)+f\ b) \quad \ldots (1)$$

$$f(a.b)=f(a).f(b). \quad \ldots (2)$$

In this case R' **will not be** said to be homomorphic image of R but we will show later that homomorphic image of R *i e.* $f(R)$ will be a **sub ring** of R'.

§ 3. Certain properties of homomorphism.

(1) *If f is a homomorphic mapping of a Ring R onto (into) a ring R' then $f(0)=0'$ where 0 and $0'$ are the additive identities of R and R' i.e.* **zero's correspond.** **(utkal 69)**

Let $a \in R$ so that $f(a) \in R'$

then $f(a)+0'=f(a)$ as $0'$ is the additive identity of R'

$=f(a+0)$ as 0 is the additive identity of R

$=f(a)+f(0)$ f is homomorphism.

Hence $f(a)+0'=f(a)+f(0)$. ...(1)

But R' being a ring is an abelian group w. r. t. addition. Hence by cancellation law from (1) we get $f(0)=0'$.

2. The image of additive inverse of $a \in R$ is additive inverse of the image of a. **(utkal 69)**

i.e $f(-a)=-f(a)\ \forall\ a \in R.$

$a \in R \Rightarrow -a \in R$ and $a+(-a)=0$

$\Rightarrow f[a+(-a)]=f(0)$

$\Rightarrow f(a)+f(-a)=0'$

where $0'$ is additive identity of R'

$\Rightarrow f(-a)$ is the additive inverse of $f(a)$

$\Rightarrow f(-a)=-f(a)$.

3. Homomorphic image of a commutative ring is commutative.

Let $a, b \in R$ $\therefore$ $ab=ba$ as R is commutative.

then $f(a)\,f(b)=f(ab)=f(ba)=f(b)\,f(a)$

$f(a), f(b) \in R'$ which therefore is commutative.

4. Homomorphic image R′ of a ring R may not be a ring with unity but if R is an integral domain then f (1) is the unity of R′, 1 being the unity of R.

$a.\,1=a=1\,a$

$\Rightarrow f(a.\,1)=f(a)=f(1.\,a)$

$\Rightarrow f(a).f(1)=f(a)=f(1).f(a)$

$\Rightarrow f(1)$ is the unity of R'.

5. If f be a homomorphism of a ring R into a ring R′ then prove that the homomorphic image f (R) of R [It will not be R′ as f is not onto] is a sub ring of R.

Let $a', b' \in f(R)$.

So that $a'=f(a), b'=f(b)$, where $a, b \in R$.

If $f(R)$ is to be a sub ring of R' then $\forall$ $a', b' \in f(R)$ we should show that

$a'-b' \in f(R)$ and $a'\,b' \in f(R)$

where $f(R)$ is a sub set of R'.

Now $a'-b'=f(a)-f(b)=f(a)+f(-b)=f\{(a+(-b)\}$

or $a'-b'=f(a-b)$.

Now $a, b \in R \Rightarrow a-b \in R \Rightarrow f(a-b) \in f(R)$

$\therefore$ $a'-b'=f(a-b) \in f(R)$.

Again $a'\,b'=f(a).f(b)=f(a.b) \in f(R)$

$\because$ $a, b \in R \Rightarrow ab \in R \Rightarrow f(ab) \in f(R)$

Hence $f(R)$ is a sub ring of R'.

§ 4. Kernel of homomorphism.

Definition. *If f is a homomorphism of a ring R onto a ring R' then the set S of all those elements of R which are mapped onto the additive identity $0'$ of R' is called the kernel of homomorphism f*

$$\therefore \quad S=\{x \in R : f(x)=0'\}.$$

Theorem 3. *The kernel of homomorphism of a ring is a two sided ideal.* **(Lucknow 69; Benares M. Sc 70)**

Given. $f: R \to R'$ $\therefore$ f is homomorphism

$$\text{Kernel of } f=S=\{x \in R : f(x)=0'\}$$

To prove. S is a two sided ideal of R.

Clearly S is a non empty sub set of R.

Let $a, b \in S \Rightarrow f(a)=0', f(b)=0'$

Now $f(a-b)=f[a+(-b)]=f(a)+f(-b)=f(a)-f(b)$

$$=0'-0'=0' \Rightarrow a-b \in S$$

Now let $r \in R$ and $a \in S$ *i.e.* $f(a)=0'$

then $f(ar)=f(a)\ f(r)=0'.f(r)=0'$

$$f(ra)=f(r).f(a)=f(r).0'=0'$$

Above relations imply that both ar and $ra \in S$.

$$\forall\ a \in S \text{ and } r \in R$$

Thus S is a two sided ideal of R.

Theorem 4. *Every quotient ring is a homomorphic image of the ring.*

Let R/S be a quotient ring of ring R and $f: R \to R/S$ where S is an ideal of R defined as

$$f(a)=S+a \ \forall\ a \in R$$

we will show that f is homomorphism.

Let $S+\alpha$, $\alpha \in R$ be an element of R/S then by definition $f(\alpha)=S+\alpha$. so that f is onto.

Again $f(\alpha+\beta)=S+(\alpha+\beta)$

$$=(S+\alpha)+(S+\beta)$$

$$=f(\alpha)+f(\beta)$$

$$f(\alpha\beta) = S+\alpha\beta = (S+\alpha)\,(S+\beta)$$
$$= f(\alpha)\, f(\beta).$$

Hence f is homomorphism of R onto R/S.

Theorem 5. *If f be a homomorphism of a field F into a ring R then the sub ring $f(F)$ of R is either a zero ring or a field isomorphic to F.* **(Lucknow 70)**

Let $f : F \xrightarrow{\text{into}} R$, then we have already shown above that $f(F)$ will be a sub ring of R.

Let S be the kernel of f then by Th. 3 S is an ideal of F. But we know that a field has no proper ideals and as such

either $S=(0)$ or $S=F$

In case $S=F$ then $f(x)=0 \quad \forall\ x \in F$

Hence $f(F)$ which is a sub ring will be zero ring.

In case $S=(0)$ then kernel will consist of 0 element only and hence the homomorphism will be an isomorphism

$f : F \xrightarrow{\text{onto}} f(F$ and f is isomorphism therefore

$F \cong f(F)$ or $f(F) \cong F$.

Theorem 6. *Every residue class ri g (i e. quotient ring) of a given ring R is a homomorphic image of the ring.*

(Raj. M. Sc. 66, 67. 69)

Let R be a given ring and S be an ideal of R so that R/S is a residue class ring whose elements are of the type

$$S+a,\ a \in R.$$

We have to prove that R/S is homomorphic image of R, For this we will show a mapping f of R onto R/S such that

$$f(a+b)=f(a)+f(b, \text{ and } f(ab)=f(a)\,f(b)$$

Consider the mapping $f: R \to R/S$ defined as

$$f(a)=S+a,\ a \in R,\ S+a \in R/S$$

The mapping onto. Corresponding to each element

$S+a$, $(a \in R)$ of R/S

$\exists\ a \in R$ such that $f(a)=S+a$

Now if $a, b \in R$ then $f(a)=S+a$, $f(b)=S+b$

$$\therefore\ f(a+b)=S+(a+b)=(S+a)+(S+b)$$
$$=f(a)+f(b)$$
$$f(ab)=S+ab=(S+a)\ (S+b)=f(a)\ f(b).$$

Hence f is a homomorphism of R onto R/S.

Theorem 7. Fundamental theorem on homomorphism converse of last theorem.

Every homomorphic image of a ring R is isomorphic to some residue class ring (quotient ring) thereof.

(Raj. M. Sc 66, 67, 69; Agra 69)

Let R be a ring and R' be its homomorphic image under f.

If S be kernel of homomorphism then S is an ideal of R and hence R/S is a residue class ring (quotient ring).

We have to prove that R/S is isomorphic to homomorphic image R' *i.e.* $R/S \cong R'$

For proving this we will have to search out a one-one onto mapping.

$$\varphi : R/S \to R'$$

which preserves the compositions in the rings.

If $a \in R$ then $S+a \in R/S$

and $f(a) \in R'$ as $f: R \to R'$

Hence in accordance with our definition

$$\phi\ (S+a)=f(a)\ \forall\ a \in R.$$

First of all we shall establish that the mapping is well defined *i.e*, independent of the particular element a chosen to represent the coset $S+a$ *i.e* if $S+a=S+b$ we will show that

$$\phi\ (S+a)=\varphi\ (S+b).$$

Now $S+a=S+b \Rightarrow a-b \in S.$

$\Rightarrow f\ (a-b)=0'$ as S is kernel of homomorphism f

$\Rightarrow f\ [(a+(-b)]=0' \Rightarrow f\ (a)+f\ (-b)=0'$

$\Rightarrow f\ (a)-f\ (b)=0'$

$\Rightarrow f\ (a)=f\ (b) \Rightarrow \varphi\ (S+a)=\varphi\ (S+b)$

Hence the mapping is well defined.

For proving φ to be an isomorphism we have to show that it is **one-one onto and preserves the compositions**

ϕ is one-one. $\varphi\ (S+a)=\varphi\ (S+b) \Rightarrow f\ (a)=f\ (b)$

$\Rightarrow f\ (a)-f\ (b)=0' \Rightarrow f\ (a)+f\ (-b)=0'.$

$\Rightarrow f\ (a-b)=0' \Rightarrow a-b \in S.$ as S is kernel

$\Rightarrow S+a=S+b \quad \therefore \quad H+a=H+b \Rightarrow a-b \in H.$

Hence φ is one-one

ϕ is onto. Let any element of R' which is homomorphic image of R be $f\ (a)$, $a \in R$ Corresponding to this element $f\ (a)$ $\exists$ a coset $S+a$ in R/S s.t. $\varphi\ (S+a)=f\ (a)$

$\therefore$ φ is onto.

φ preserves ring compositions.

$\varphi\ [(S+a)+(S+b)]=\varphi\ [S+a+b]=f\ (a+b)$

$=f\ (a)+f\ (b)=\varphi\ (S+a)+\varphi\ (S+b)$

$\varphi\ [(S+a)\ (S+b)]=\varphi\ (S+ab)=f\ (ab)$

$=f\ (a)\ f\ (b)=\varphi\ (S+a)\ \varphi\ (S+b)$

Hence φ is an isomorphism of

R/S onto R' *i.e.* $R/S \cong R'$

Theorem 8. *S and T are two ideals of a ring R such that $S \subset T$ then the quotient ring T/S is an ideal of quotient*

ring R/S and conversely if T/S is an ideal of R/S then T is an ideal of R such that $S \subset T$.

Frst of all we should note the criteria for S to be an ideal of R

(1) S is a sub set of R

(2) $\forall\ a, b \in S, a-b \in S$

(3) $rs \in S, sr \in S\ \forall\ r \in R\ \forall\ s \in S$ § 20. P. 246.

Proof. S is an ideal of R and hence R/S is a quotient ring.

Let us now verify if T/S is a quotient ring or not

$$S \in T \subset R$$

S is and ideal of R.

Now $rs, sr \in S\ \forall\ r \in R$ and $\forall\ s \in S$

$\Rightarrow\ rs, sr \in S\ \forall\ r \in T$ and $s \in S\ \because\ T \subset R$

Above relation shows that S is an ideal of T. Hence T/S is a quotient ring.

Now we have to prove that T/S is an ideal of R/S for which we shall prove properties (1), (2) and (3) written above.

(1) $T/S \subset R/S$

Any element of T/S is $S+a$ where $a \in T$ Since $T \subset R\ \therefore\ a \in R$

and in this case $S+a \in R/S\ \therefore\ T/S \subset R/S$

(2) $S+a, S+b \in T/S$

where $a, b \in T$ or $a-b \in T$ as T is an ideal

$$\therefore\ (S+a)-(S+b)=(S+a)+(-1)\ (S+b)$$
$$=(S+a)+(S-b)$$
$$=S+(a-b) \in T/S \text{ as } a-b \in T$$

(3) $(S+a) \in T/S\ \ (a \in T)$

$(S+r) \in R/S\ \ (r \in R)$

$\Rightarrow (S+a)\ (S+r)=S+ar \in T/S$ where $ar \in T$ as T is an ideal.

Similarly $(S+r)\,(S+a) \in T/S$

Hence T/S is an ideal of R/S.

Converely.

Given : Quotient ring T/S is an ideal of quotient ring R/S *i.e.* all the three criteria are satisfied

i.e. $T/S \subset R/S$ and S is an ideal of $T \quad \therefore \quad S \subset T$

To prove that T is an ideal of R such that $S \subset T$ for this we will establish criteria no. 1, 2, 3 given above

(1) $T \subset R$

Let $t \in T \Rightarrow S+t \in T/S$

$\Rightarrow S+t \in R/S$ as $T/S \subset R/S$ by (i)

$\Rightarrow t \in R$

Since $t \in T \Rightarrow t \in R \quad \therefore \quad T \subset R.$

Also $S \subset T \therefore S \subset T \subset R.$

(2) $a, b \in T \Rightarrow a-b \in T$

$a, b \in T \Rightarrow S+a, S+b \in T/S$

$\Rightarrow (S+a)-(S+b) \in T/S$ as T/S is an ideal

$\Rightarrow S+(a-b) \in T/S$

$\Rightarrow a-b \in T$

(3) $t \in T, r \in R \Rightarrow tr \in T, rt \in T$

$S+t \in T/S$, $S+r \in R/S$ and as T/S is an ideal of R/S

$\therefore \quad (S+t)\,(S+r)$ and $(S+r)\,(S+t) \in T/S$

or $S+tr$ and $S+rt \in T/S$

or tr and $rt \in T.$

Since all the three criteria for T to be an ideal are satisfied and as such T is an ideal of R.

CHAPTER VIII
EUCLIDEAN DOMAIN

§ 1. Euclidean Domain.

Definition *An integral domain D (i.e. a commutative ring with unity and without zero divisors) is called a Euclidean ring if there exists a mapping f (Valuation function) of the set of all non zero elements of D into a set of non negative integers.*

{i e. $f : D_0 \to A$ where A is a set of non negative integers} satisfying the following.

(a) $\forall\ a, b \in D_0$ *i e. non zero elements of D*

$$f(a) \leqslant f(ab).$$

(b) $\forall\ a, b \in D_0$ *i e. non zero elements of D* $\exists\ q$ *and r in D such that*

$$a = bq + r$$

where either $r = 0$ or $f(r) < f(b)$.

(Raj. 67; Meerut 69, 70; Gujarat 70: Delhi 70)

The above is known as **Division Algorithm.**

Notation. A euclidean domain is denoted as $[D, +, ., f]$

Corresponding to a given non zero element $a \in D$, $f(a)$ is called f value of a and this should be **some non negative integer** for every non zero element of D

for $a = 0$, $f(a)$ remains undefined.

Exercise 1

1: *Prove that the ring I of integers is a Euclidian domain* I_0 *is the set of non zero integers of I.*

Define $f : I_0 \to A$ when A is a set of non negative integers such that $f(x) = |x|\ \forall\ x \in I_0$ *i.e.* $x \neq 0$

Clearly $|x|$ is a non negative integer $\in A$;

Also $f(-5) = |-5| = |5|$ which is non negative integer

If $a, b \in I_0$ then $f(a) = |a|$, $f(b) = |b|$,

Also when $a, b \in I_0$ then ab also belongs to I_0 as it will be non zero.

Since a and b are non zero, the given ring is a ring without zero divisors.

$\therefore \quad f(ab)=|ab|$

Now $|a| \leqslant |a|\,|b| \leqslant |ab|$

or $\quad f(a) \leqslant f(ab).$ ...(1)

Again by division algorithm in I we know that $\exists$ integers q and r in I such that

$$a=bq+r \text{ where } 0 \leqslant r < |b|$$

i.e. either $r=0$ or r is $a+$ive integer less than $|b|$

or $\quad r < f(b).$

But when r is $+$ive integer then $f(r)=|r|=r.$

Hence either $r=0$ or $f(r) < f(b)$ ...(2)

From 1 and 2 we conclude that both the conditions of euclidean domain are satisfied and as such ring of integers I is a euclidean domain.

2. *The integral domain of Gaussian integers is euclidean domain.* **(Meerut 70; Delhi 70; Gujarat 70; Raj. M.Sc. 1967)**

Refer Ex. 5 P 199. $a+ib$ is a gaussian integer where a and b are integers and the set of all gaussian integers is an integral domain.

Let G_0 be the set of all non zero gaussian integers.

$$\alpha=a+ib,\ \beta=c+id \in G_0.$$

$$\alpha\beta=(ac-bd)+i(ad+bc) \in G_0$$

Let $f: G_0 \to A$ where A is a set of non negative integers such that $f(\alpha)=f(a+ib)=a^2+b^2,\ f(\beta)=c^2+d^2$

We shall now verify the properties of euclidean domain.

$$f(\alpha\beta)=(ac-bd)^2+(ad+bc)^2$$

$$=a^2c^2+b^2d^2+a^2d^2+b^2c^2$$

$$=(a^2+b^2)\,(c^2+d^2)$$

$$=f(\alpha)\,f(\beta).$$

Since $f(\alpha)=a^2+b^2 \geqslant 1$, $f(\beta)=c^2+d^2 \geqslant 1$.

Hence it follows from above that

$$f(\alpha) \leqslant f(\alpha\beta) \qquad \ldots(1)$$

Thus the first condition is satisfied.

We have now to verify the second condition.

Let λ be a complex number defined as

$$\lambda=\frac{\alpha}{\beta}=\frac{a+ib}{c+id}=\frac{(a+ib)\,(c-id)}{c^2+d^2}=p+iq \text{ say}$$

where p and q are rational numbers and thus λ is not necessarily a gaussian integer.

Now choose p' and q' integers which are nearest to rational numbers p and q.

$\therefore \quad |p-p'| \leqslant 1/2, |q-q'| \leqslant 1/2$

Choose $\lambda'=p'+iq'$ where p' and q' are integers and as such λ' is a gaussian integer.

Now $(\lambda-\lambda')\,\beta=\lambda\beta-\lambda'\beta=\alpha-\lambda'\beta$.

Since α, β, λ' are gaussian integers, it follows that $(\lambda-\lambda')\,\beta$ is also a gaussian integer.

Also $f((\lambda-\lambda')\,\beta)=f[\{(p-p')+i\,(q-q')\}\,(c+id)]$

$$=[(p-p')^2+(q-q')^2]\,[c^2+d^2]$$

$$\leqslant [\tfrac{1}{4}+\tfrac{1}{4}]\,f(\beta)=\tfrac{1}{2}\,f(\beta) < f(\beta)$$

$\therefore \quad f((\lambda-\lambda')\,\beta) < f(\beta)$.

But $\alpha=\lambda\beta=\lambda'\beta+(\lambda-\lambda')\,\beta$.

where $f((\lambda-\lambda')\,\beta) < f(\beta)$

or $(\lambda-\lambda')\,\beta=0$ as when p and q are integers then $p-p'=0$, $q-q'=0$, by choice of p' and q' and hence $\lambda-\lambda'=0$

$\therefore \quad (\lambda-\lambda')\,\beta=0$

Thus we prove that $a=bq+r$.

where either $r=0$ or $f(r) < f(b)$.

Here $r=(\lambda-\lambda')\,\beta$, $b=\beta$, $a=\alpha$, $q=\lambda'$

Therefore the domain of gaussian integers is a euclidean domain.

3. *Everey field is a euclidean domain.*

Let $f : F_0 \to A$ where F_0 is the set of non zero elements of F such that $f(a)=0 \ \forall \ a \in F_0$

Thus the mapping f assigns the integer zero to every non zero element of F.

If $a, b \in F_0$ then $ab \in F_0 \quad \therefore \quad f(ab)=0=f(a)$

$\therefore \quad f(a)=f(ab)$ and it proves condition *I*

Again since F is a field every non zero element is inversible *i.e.* $b\neq 0$, b^{-1} exists such that $bb^{-1}=1$

Now $a=(ab^{-1})\, b+0$

Thus $a=bq+r$ where $q=ab^{-1}$ and $r=0$

Hence the second condition is also satisfied.

Therefore every field is a euclidean domain.

4. *Let F be a field and x be an indeterminate, then the polynomial domain F [x] over F is a euclidean domain.*

Let $f(x)$ be a non zero polynomial in $F[x]$ and we define a mapping f on non zero polynomials to a set of non negative integers such that

$f(a)=\deg f(x) \ \forall \ f(x)\neq 0 \in F[x]$.

where $\deg f(x)$ is certainly a non zero negative number.

Let $a=f(x)$ and $b=g(x)$.

Again if $f(x)$ and $g(x)$ be both non zero polynomials in $F[x]$ then $\deg [f(x)\, g(x)]=\deg f(x)+\deg g(x) \geqslant \deg f(x)$

$\because \quad \deg g(x) \geqslant 0$

$\therefore \quad f(ab) \geqslant f(a)$ or $f(a) \leqslant f(ab)$

Thus the first condition is satisfied.

Also by division algorithm § 30 P. 272, there exists unique polynomials $q(x)$ and $r(x)$ in $F[x]$ such that

$f(x)=g(x)\, q(x)+r(x)$ where

$r(x)$ is either zero or of degree less than that of $g(x)$ or degree $r(x) \leqslant \deg g(x)$

or $\quad f(r(x)) \leqslant f(g(x))$

Thus the second condition is also satisfied

Hence the ring of polynomials over a field is an euclidean domain.

Theorem 1. *Every euclidean domain is a principal ideal domain.* **(Gujarat 70; Aligarh 65; Raj. M.Sc. 67; Meerut M. Sc. 69)**

Let D be an euclidean domain and S be any arbitrary ideal of D. If S is a null ideal then $S=(0)$ which we know is a principal ideal (See **Page 256**).

Now let us suppose that S is not a null ideal so that there exist elements in S which are not zero. Choose $b\neq 0$ to be an element in S such that $f(b)$ (which is a non negative number) is least. In other words it means that there is no number $c\neq 0$ in S such that $f(c) < f(b)$. We will establish that the ideal S is generated by b *i e.* $S=(b)$ and hence S is a principal ideal.

Let a be any other element of S then since D is an euclidean domain $\exists$ elements q and r in D such that

$a=qb+r$ where either $r=0$ or $f(r) < f(b)$.

Now S is an ideal $\therefore\ q \in D, b \in S \Rightarrow qb \in S$ by def. of ideal.

Again $a \in S, qb \in S \Rightarrow a-qb=r \in S$.

Also either $r=0$ or $f(r) < f(b)$.

In case $r\neq 0$ then $f(r) < f(b)$ which contradicts the supposition that b is that element of S such that $f(b)$ is least and no other element c of S is such that $f(c) < f(b)$. Hence we must have $r=0$

In that case $a=qb$, which shows that every element a of S is a multiple of b.

$\therefore \quad a \in S \Rightarrow a \in (b) \qquad \therefore S \subset (b). \qquad \ldots(1)$

Again if xb be any element of (b) then $x \in D$.

But $x \in D, b \in S \Rightarrow xb \in S$

$\therefore \quad x\,b \in (b) \Rightarrow xb \in S \therefore (b) \subset S$

From 1 and 2 we conclude that $S=(b)$, *i.e.* any ideal S is generated by single element b and as such it is a principal ideal. Therefore D which is an euclidean domain is a principal ideal ring.

Theorem 2. *Prove that every euclidean domain possesses unity element.*

Let D be an euclidean domain, then D is an ideal of D which is a principal ideal. Hence there exists an element $b \in D$ such that $D=(b)$ *i.e.* every element of D is a multple of b. Again since b is also an element of D it follows that b is also a multiple of b *i.e.* there exists an element $c \in D$ such that $b=bc$. ...(1)

Choose a any other element of D then a is also a multiple of b *i.e.* $\exists$ an elrment x in D such that $a=bx$

$$\therefore \quad ac=(bx)\ c=(bc)\ x \quad \because \ R \text{ is commutative.}$$
$$=bx \qquad \because \qquad bc=b$$
$$=a \qquad \because \qquad a=bx$$

Hence $ac=a=ca \ \forall \ a \in D$

Thus c is the unity element.

§ 2. Greatest Common Divisor.

We have defined divisibility in an integral domain in § 16 P. 227 as a/b *i.e.* a divides b if there exists an element $c \in D$ such that $b=ac$. We have also proved that the relation of divisibility is reflexive as well as transitive.

Further we defined that two non-zero elements a, o in D are associate if each is a divisor of the other *i.e.* a/b and b/a, and this is expressed as $a \sim b$. See P. 229. and two elements a and b in an idtegral domain are associates if one is a unit times the other. See P. 230.

Again we have proved that the relation of being associates is an equivalance relation. See. Th. 12 P. 229.

Now consider two elements 54, 12, their greatest common divisor is 6.

i e. 6/54, 6/12.

Also 3 divides both 54, 12 *i.e.* 3/54, 3/12.

but 3 is a divisor of 6 *i.e.* 3/6

i.e. 6 is a greatest divisor if 6 divides both 54 and 12 and if there be any other divisor of 54 and 12 then it should be a divisor of 6.

Definition of greatest common divisor.

Let a, b be two non zero elements of D, then an element g is said to be greatest common divisor of a and b if,

(*a*) g/a, and g/b.

(*b*) $h/a, h/b \Rightarrow h/g$.

The first relation implies that g divides both a and b, the second relation implies that if there be any other element h which divides both a and b then it also divides g *i.e.* it is a factor of g so that g becomes greatest common divisor.

Notation The greatest common divisor of a and b is expressed symbolically as (a, b).

Existence of greatest common divisor.

Theorem 3. *Let D be a euclidean domain and a, b be any two non zero elements of D. Then a and b have a greatest common divisor d which can be expressed in the from*

$$d=\lambda a+\mu b \text{ for some } \lambda, \mu \in D.$$

Consider the set $S=\{sa+tb : s, t \in D\}$

We shall show that S is an ideal of D *i.e.* it satisfies both the conditions of being an ideal of a commutative ring.

$x-y \in S \ \forall \ x, y \in S$.

and $rx \in S \ \forall \ r \in D$ and $\forall \ x \in S$ **Page 245–47**

Let $x \in S=s_1a+t_1b, s_1, t_1 \in D$

$y \in S=s_2a+t_2b, s_2, t_2 \in D$

$x-y=(s_1-s_2)\,a+(t_1-t_2)\,b=sa+tb \in S$

because s_1-s_2 and t_1-t_2 both belong to D.

Again if r be any element of D and x be any element of S then $rx=r\,(s_1a+t_1b)=(rs_1)\,a+(rt_1)\;b \in S$

Hence S is an ideal of D.

We have proved in Th. 2 P. 475 that every euclidean domain is a principal ideal domain *i e.* every ideal is a principal ideal. Hence S is a principal ideal, *i e.* an ideal generated by a single element. In other words it means that there exists an element d in S such that every element in S is a multiple of d.

Now d being an element of S it follows from definition of S that $\qquad d=\lambda a+\mu b$ for some $\lambda, \mu \in D$

Since D is a ring with unity then putting $s=1, t=0$ we get.

$1\cdot a+0\cdot b=a \in S$. Similarly putting $s=0, t=1$ we get
$0\cdot a+1\cdot b=b \in S$

But every element in S is a multiple of d $\therefore$ $d\,|\,a$, $d\,|\,b$

Now if both a and b are divisible by any other element d' *i.e.* $d'|a$, $d'|b$, then $d'|a \Rightarrow d'|\lambda a$, $d'|b \Rightarrow d'|\mu b$

so that $d'|\lambda a+\mu b$ or $d'|d$.

Hence we have

(a) $d|a$, $d|b$

(b) $d'|a, d'|b \Rightarrow d'|d$.

Therefore $d=\lambda a+\mu b$ is the greatest common divisor of a and b.

§ 3. Relatively prime elements of a euclidean domain.

We know that 5, 17 are prime relatively and their greatest common divisor is 1 *i.e.* $(5, 17)=1$. Now choose 10 any other integer $5/17\times 10$ then $5/10$ *i.e.* 5 divides 10

Definition. *Two elements a, b of an euclidean domain are said to be* **co prime** *or relatively prime if their g.c.d is 1 i.e. if $(a, b)=1$.*

Theorem 4. *Let a, b, c be any three elements of an euclidean domain D such that $(a, b)=1$ i.e. greatest common divisor of a and b is 1, then if a/bc i e. if a divides bc then a/c i.e. a divides c.*

We know that if d be the greatest common divisor of a,b then there exists λ, μ in D such that

$$d=\lambda a+\mu b$$

$$\therefore \quad 1=\lambda a+\mu b \text{ as } d=1 \qquad \ldots(1)$$

Multiplying both sides by c we get

$$c=\lambda ac+\mu bc \qquad \ldots(2)$$

we are given a/bc *i.e.* a divides $bc \Rightarrow \exists\ q \in D$ such that

$$bc=qa$$

$$\therefore \quad c=\lambda ac+\mu qa \text{ from (2)}$$

or $$c=(\lambda c+\mu q)\, a$$

Above relation shows that a is a divisor of c *i.e.* a/c.

Theorem 5. *Let a, b be any two elements of euclidean domain D and p be any prime element of D such that p/ab, then p divides at least one of a or b.*

Suppose p does not divide a which in other words mean that p and a are relatively prime *i e.* $(p, a)=1$, Since p/ab and $(p, a)=1$, it follows from last theorem that p/b *i.e.* p divides b

Cor. If p is a prime element in D and p divides the product of $a_1, a_2, \ldots, a_n$ of elements in R, then p divides at least one of $a_1, a_2, \ldots, a_n$.

Theorem 6. *Let $(D, +, ., f)$ be a euclidean domain and a be a non zero element of D then a is a unit if and only if $f(a)=f(1)$.*

Ist case Let a be a unit $\Rightarrow \exists\ a^{-1}$ in D such that $a\,a^{-1}=1$

$$\therefore \quad f(a\,a^{-1})=f(1).$$

But $f(a\,a^{-1}) \geqslant f(a)$ by def. of D.

$$\therefore \quad f(1) \geqslant f(a). \qquad \ldots(1)$$

Again $f(1.a) \geqslant f(1)$...(2) by def. of D.

From 1 and 2 we conclude that $f(a)=f(1)$.

2nd Case. Let $f(a)=f(1)$ and we will show that a is a unit in D.

Now by second property of euclidean domain there exist q, r in D such that $1=aq+r$ where either $r=0$

or $f(r) < f(a)$ or $f(r) < f(1)$.

Now $1.r=r$ and $f(ab) \geqslant f(a)$,

$\therefore$ $f(1.r) \geqslant f(1)$ or $f(a) \geqslant f(1)$.

Since $f(r) \geqslant f(1)$ therefore the possibility of $f(r) < f(1)$ is ruled out.

Hence we must have $r=0$ $\therefore$ $1=aq$ or $a/1 \Rightarrow a$ is a unit.

Theorem 7. *Let $(D, +, .)$ be a euclidean domain and a, b be two non zero elements of D, then*

(1) $f(ab)=f(a)$ if b is a unit.

(2) $f(ab) > f(a)$ if b is not a unit.

(Meerut M Sc. 1967, 70)

Since $a, b \in D$ we have from definition of D

$$f(ab) \geqslant f(a) \qquad (1)$$

(1) Let b be a unit in D so that b^{-1} exists.

$\therefore$ $a=(ab)\,b^{-1}$ or $f(a)=f((ab)\,b^{-1})$

But $f((ab)\,b^{-1}) \geqslant f(ab)$ from I.

or $f(a) \geqslant f(ab)$ ...(2)

Hence from 1 and 2 we conclude that

$$f(ab)=f(a)$$

(2) Let b be not a unit in D. Again a, b are non zero elements of D and D is without zero divisors it follows that $ab \neq 0$, Since a and ab are both non zero elements of D we get from definition of D.

$a=q(ab)+r$ with $q, r \in D$ such that

either $r=0$ or $f(r) < f(ab)$.

Now if $r=0$ then $a=q(ab) \Rightarrow a-q(ab)=0$

$\Rightarrow a(1-qb)=0 \Rightarrow 1-qb=0$ as $a\neq 0$ and D is without zero divisors.

$\Rightarrow qb=1 \Rightarrow b/1 \Rightarrow b$ is a unit which is a contradiction to the fact that b is not a unit. Hence r cannot be zero so we must have

$$f(r) < f(ab) \quad \text{or} \quad f(ab) > f(r) \qquad \ldots (3)$$

Now $a=q(ab)+r \Rightarrow r=a(1-qb)$

$\therefore \quad f(r)=f(a(1-qb)) \geqslant f(a)$ by def. of D. ...(4)

Hence from (3) and (4) we get $f(ab) > f(a)$.

§ 4 Unique factorization Theorem

We know that in the case of integers every non zero integer is either a unit or can be writt.n as the product of a finite number of primes which is unique in the sense that if

$a=p_1p_2 \quad p_n=q_1q_2\ldots q_m$ where p_i' and q_j' are primes then $n=m$ and on proper numbering p_i is an associate of q_i

We shall now prove a similar theorem for euclidean domain.

Theorem 8 Unique Factorization Theorem in the euclidean domain.

Statement: Ist part. *Let $(D, +, ., f)$ be an euclidean domain then every non zero element a in D is either a unit or can be written as the product of a finite number of prime elements of D.*

2nd part. *The obove product of primes is unique in the sense that if $a=p_1p_2\ldots p_n=q_1q_2\ldots q_m$, where $a\neq 0$, $a\neq$unit where p_i' and q_j' are prime elements of D then $n=m$ and each p is an associate of some q and each q is an associate of some p.*

Proof. Ist part. Let a be a non zero element of D. If a is a unit then there is nothing to prove. Also when a is a unit then $f(a)=f(1)$ Th. 6 P. 478.

If a is not a unit then we have to show that a can be expressed as the product of a finite number of elements. We shall prove the theorem by induction on $f(a)$.

Assume that the theorem is true for all $x \in D$ such that $f(x) < f(a)$. and then we shall prove the theorem for a.

Now if a is prime then the theorem is proved but if a be not prime then a is composite and let $a = bc$ where $b, c \in D$ and both are non units

Now by Th. 7 P. 479 $f(b) < f(bc)$ or $< f(a)$ $\because$ $bc = a$.

$f(c) < f(bc)$ or $< f(a)$ $\because$ $bc = a$

Since both $f(b)$ and $f(c)$ are less then $f(a)$ therefore by Induction hypothesis we can write b and c as tne produot of a finite number of elements of D.

$\therefore$ $b = p_1 p_2 \cdots p_k$, $c = q_1 q_2 \cdots q_r$

$\therefore$ $a = bc = p_1 p_2 \cdots p_k . q_1 q_2 \cdots q_r$.

Hence a has been expressed as the product of a finite number of prime elements of D.

2nd part. Let $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$

From above we observe that p_1 is a divisor of $p_1 p_2 \cdots p_n$ and hence it follows that p_1 is a divisor of $q_1 q_2 \cdots q_m$, Therefore by Th. 4 Cor. P. 478 p_1 must divide at least one of $q_1, q_2 \cdots q_m$. Let us suppose that p_1 divides q_j but p_1 and q_j are both prime elements in D and hence p_1 and q_j must be associates. Therefore $q_j = u_1 p_1$ where u_1 is a unit in D.

$\therefore$ $p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_j \cdots q_m = u_1 p_1 q_1 q_2 \cdots q_{j-1}, q_{j+1} \cdots q_m$

cancelling $p_1 \neq 0$ from both sides we have

$$p_2 p_3 \cdots p_n = u_1 q_1 q_2 \cdots q_{j-1} q_{j+1} \cdot q_m. \qquad \ldots(2)$$

We can repeat the same argument on p_2 as on p_1 and we will have $p_3 p_4 \cdots p_n = u_1 u_2 q_1 q_2 \cdots q_{j-1} q_{j+1} q_{k-1} q_{k+1} \cdots q_m$ where u_2 is a unit in D.

After repeating the above step n times the left hand side will be reduced to 1 and the right hand side will be the pro-

duct of some units in D and some q^s (number of which will be excess of m over n). But q^s are prime elements of D and as such they are not units. Now as the product of certain units and certain q^s which are prime in R.H.S. cannot be equal to 1 in L.H S. therefore m cannot be greater than n *i.e.* $m \leqslant n$. Similarly interchanging the roles of p^s and q^s we will have $n \leqslant m$ and hence $m=n$.

Also we have shown that every p is an associate of some q and conversely every q is an associate of some p. Thus the 2nd part of the theorem is completely proved.

UNIVERSITY PAPERS SOLVED

Allahabad 1970

1. (a) Show that in a group, cancellation laws hold. Will a semi-group, in which cancellation laws hold, be a group ?

Discuss the case when n is finite.

(b) Show that the set u_n of nth roots of unity forms a cyclic group with respect to multiplication.

Prop. 4, P. 46, Prop 10, P 50, Q. 19 P 24.

2. (a) What do you understand by the statement :— "When two groups are isomorphic then in some sense they are equal."

(b) Show that isomorphism of a group maps the dentity into the identity and the inverse of an element into the inverse of its image.

(c) Let $R(x)$ be the set of polynomials over the set of real numbers. Prove that $R(x)$ is a group with respect to addition.

Th. 15 P. 110, § 17 P. 108, Th. 30 P. 267.

3. (a) Define an ordered integral domain. Show that the unity element of an ordered integral domain I is a +ve element of I and prove that the set of complex numbers is not an ordered integral domain.

(b) Give, without proof, an example of an integral domain which contains only five elements. Is this an ordered integral domain ? Give reasons.

§ 15 P. 224, Ex. 1, 2, 3 P. 225.

4. (a) If $g(x)$ $(\neq 0)$ and $f(x)$ are any two polynomials over a field F, show that there exist unique polynomials $q(x)$ and $r(x)$ over the field F such that $f(x)=q(x).g(x)+r(x)$, where, $r(x)$ is either zero or of degree less than the degree of $g(x)$.

(b) Find the zeros of the polynomials $x^4+2x^3-21x^2-22x+4$ if they are in arithmetical progression.

§ 30, P. 272, See author's book on Theory of equations.

5. (a) Define a ring. Prove that the set of residue classess modulo the +ve integer m is a ring with respect to addition and multiplication of residue classes mod (m).

(b) Prove that in a field :—

(i) $(a/b)-(c/d)=(ad-bc)/bd$;

(ii) $(-a)^{-1}=-(a^{-1})$:

(iii) $(-a)/(-b)=a/b$.

Q. 4 P. 173.

Gorakhpur 70

1. (a) Show that the non-zero residue classes modulo a positive prime integer p form a commutative group with respect to multiplication of residue classes as the binary operation.

(b) Define the order of an element in (i) additive group, (ii) a multiplicative group. What is the order of 3 in multiplicative group of non zero residue classes modulo 5.

Th. 4 P. 43, § 12 P. 79, see 5 P. 81.

2. (a) State and prove the necessary and sufficient conditions for a complex H to be a subgroup of the group G.

(b) Define alternating group Show that the alternating group A_n is a subgroup of symmetric group S_n of the permutations over n objects. Write down all the proper subgroups of S_3.

§ 3 P. 131, Th. 8 p. 71

3. (a) Prove that the relation of isomorphism in set of all groups is an equivalence relation.

(b) If R be the additive group of real numbers and R^+ be the multiplication group of positive real numbers. Prove that the map $f: R \to R^+$ given by $f(x)=e^x$, $x \in R$ is an isomorphism.

Th. 15 P. 110, Ex. P. 96

4. (a) Distinguish between the order of the group and order of an element in a group. Prove that if $a, p \in G$ then a and $p^{-1} a p$ have the same order in G.

(b) If G is a cyclic group of order n generated by an element a, then prove that G is generated by a^m $(m < n)$ if and only if m is prime to n.

Th. 13 P. 83, Th. 24 p. 127.

5. (a) State and prove Lagrange's theorem on the order of sub-groups of a group. Show that every group of prime order is cyclic.

(b) State the definitions of a field and integral domain and give suitable illustration for each.

§ 11 p. 161, § 5 p. 192, § 6 p. 195 and examples on p. 193 and p. 196,

Kanpur 1970

1. (a) Are the following sets a l equal ?

A=$\{x : x$ is a letter in the word reap$\}$.

B=$\{x : x$ is a letter in the word paper$\}$

C=$\{x : x$ is a letter in the word rape$\}$.

(b) Show that the set of whole numbers (including zero) with addition composition is an infinite group.

(c) Define the concept of group in the additive termino logy. If corresponding to any element a of a group G there is an element 0_a which sati.fies one of the conditions $a+0_a=a$ or $0_a+a=a$, then show that it is necessary that 0_a 0

See set theory, Ex. 1 p. 8, prop 6 p 47.

2. (a) A subgroup H of a cyclic group G is also cyclic and generated by a^m, where a is a generator of G and m is least positive integer such that $a^m \in H$.

(b) Prove that the relation congruence modulo m is an equivalence relation in the set of integers.

Th 9 p. 146, See set theory book.

3. (a) Prove Lagrange's theorem that the order of a subgroup H of a finite gr ›up G is a divisor of the order of the group G.

(b) Prove that every finite group of composite order possesses proper subgroup.

§ 11 p. 161 , cor. 5 p. 164.

4. (a) Is every field al‹o a ring ? Do the set of all integers under usual addition and multiplication form a field ? Give r‹asons to support your answer.

(b) Prove that the set I ($\sqrt{2}$) of real numbers of the from $m+n\sqrt{2}$, where m, n are integers is a ring with ordinary addition and multiplication.

Q I (a) P. 169, Q. 2 p. 170.

5. (a) What do you mean by a vector space ? Give two examples.

(b) Show that the sets S of vector $\alpha_1=(1, 2, 1)$, $\alpha_2=(3, 1, 5)$. $\alpha_3=(3, -4, 7)$ is linearly dependent. Also find the maximum linearly independent subsets of S.

§ 2 p, 285, Proced as in I (b) p. 322.

Lucknow 1970

1. (a) Define a subgroup of a group. Show that a non-empty complex H of a finite group G is a sub group, if and only if, it is closed with respect to multiplication.

(b) Show that a poper sub-groups of the multiplicative group $G=\{1, -1, i, -i\}$ is $H=\{1, -1\}$. Are there others ? Give reasons for your answer.

§ 1 p. 129, Th. 3 p. 134, Th. 11 p. 147 Ex. p. 148.

2. (a) If H is a sub-group of G, where the orders of these groups are h and g respectively, prove that h is a factor of g.

(b) Define a cyclic group. Show that group of prime order is necessarily cyclic.

§ 11 p 161, cor. 4 p. 163.

3. (a) Define a ring and an integral domain. If R is a ring with zero element z, then prove that for all $a \in R$, $a.z=z.a=z$.

(b) Define a vector space. In a vector space V over a field F with 0 the zero element of F and **0** the zero element of V prove that

(i) $a.\mathbf{0}=\mathbf{0}$ for all $a \in F$; (ii) $0.\alpha=0.$ for all $\alpha \in V$

§ 1 p. 168, § 2 (A) p. 176, § 2 p. 285, § 3 p. 296.

Meerut 1970

1. (a) Define mappings :—

Consider the mapping f defined by $f : I \to I$,

where $f(x)=n-(-1)^n$, $n \in I$ is the set of natural numbers.

(b) What are equivalent relation ? In the set of all triangles in a plane, show that the relation of congruence (or similarity) is an equivalence relation.

See set theory.

2. (a) Prove that the intersection of two subgroups of a group G is also a subgroup of G.

(b) Every subgroup of a cyclic group G is cyclic.

§ 4 p. 140, Th. 9 p. 146.

3. (a) Distinguish between the order of a group and the order of an element in a group. Prove that the order of an element of a finite group is a divisor of the order of the group. Deduce that if a be an element of a finite group G of order N, then $a^N = e$, where e is the identity of G.

(b) If a group G is homomorphic to a group G under a homomorphism ϕ, then G is isomorphic to the factor group G/H where H is the kernel of ϕ.

§ 12 p. 79, Th. 12 p. 82, Th. 5 p. 436.

4. (a) State the definitions of a field and an integral domain and give suitable illustrations for each.

(b) The set M of all 2×2 matrices of the form $\begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix}$ for a, b integers is a right ideal but not a left ideal in the ring R of all 2×2 matrices with elements as integers. Here N is the subset of R consisting of these elements whose first column contains only zeros.

§ 5 p. 193 § 6 p 195, Q. I p. 270.

5. (a) Prove that any two bases of a finite dimensional vector space have the same number of elements.

(b) Suppose V is a finite dimensional vector space and S and T are two subspaces of V then prove that,

$$\dim (S+T)=\dim S+\dim T-\dim (S\cap T)$$

Th. 11 p. 338, Th. 17 p. 349.

Saugar 1970

1. (a) What is a group ? Prove that the order of every sub-group of a finite group G is a divisor of the order of G.

(b) Show that the set of even integers is a subgroup of the additive group of integers.

§ 11 p 161, Ex. I p. 133.

2. (a) Define a cyclic group and show that all subgroups of a cyclic group are cyclic.

(b) Prove that every group of order n is isomorphic to a permutation group of n elements.

Th. 9 p. 146, Th. 17 p. 114.

3. (a) Define a ring and show that the set of integers is a commutative ring with unit element.

(b) Give an example of a ring which is not an integral domain.

§ 1 p. 168, Ex. I p. 169, See 6 p. 193 .

4. (a) What is a field ? Give two examples.

(b) Find a polynomial whose zeros are k times the zeros of a given polynomial $f(x)$ over a field F.

§6 p 195 and examples p. 196. See Theory of equations.

5. If α, β, γ be the zeros of the polynomial $f(x)=x^3+qx+r$ over a field F, obtain the polynomial whose zeros are $(\alpha-\beta)^2$, $(\beta-\gamma)^2$. $(\gamma-\alpha)^2$.

See theory of equations book.

Allahabad 1971

1. (a) A semi-group G in which equations $ax=b$ and $ya=b$ are solvable, for any a and b in G, is called a group. Show that in such a group there exists a unique 'unit' element e satisfying $ae=a=ea$, for every $a \in G$, and for each element a of G, there exists a unique 'inverse' element a' such that

$$a'a=e=aa'.$$

(b) Giving reasons in support of your answer, examine if the following sets form a group :—

(i) Set of even integers, with respect to addition.

(ii) Set of odd integers, with respect to addition,

(iii) Set of integers, with respect to sub-traction.

Prop § 10. P. 50, see 3. 4, 6, P, 9, 10

2. (2) Explain the terms homomorphism, isomorphism, endomorphism and automorphism in relation to groups, giving an example of each.

(b) Show that if A and B are normal sub-groups of a group G, then so is $A \cap B$.

§ 16 p, 94, § 1 p. 431. see 6 p. 441, § 4 p. 442

Th. 4 p. 406

3. (a) When $a, b \in I$ define

$a+b=a+b+1$, and

$a \times b=a+b+ab$,

show that I is a commutative ring with respect to + and ×. What is the zero of the ring ? Does it have a unit element ?

(b) Prove that a ring R is without zero divisors if the restricted cancellation law holds in R.

Refer Ex. 7 p. 188, Th. 1 p. 192

4. (a) Prove that from the elements of an integral domain it is possible to construct a field, called the Quotient Field of the integral domain.

(b) Prove that $1, -1, i, -i$ are the units of the integral domain of complex number of the form $a+ib$ (a, b being integers).

§ 19 p. 236, Q. 3 p 228

10 (a) Define the zeros of a polynomial and show that a palynomial.

$f(x) \equiv a_0+a_1x+a_2x^2+\ldots\ldots+a_nx^n$, $a_n \neq 0$, over the field of complex numbers has exactly n zeros which are complex numbers.

(b) Prove that if $p(x)$ is an irreducible polynomial over a field F and if $p(x)$ divides the product $f(x).g(x)$ of two polynomials over F, then $p(x)$, divides $f(x)$ or $p(x)$ divides $g(x)$.

see p. 272,

Lucknow 71

1. State the axioms of a group. Under what conditions can we say that a subset of it becomes a subgroup, and illustrate by an example.

Prove that if H is a subset of a group G then a necessary and suffcient condition for it to become a subgroup is that the following conditions be satisfied :—

(i) The composition of any two elements of H is an element of H

(ii) The inverse of every element of H is an element of H

(iii) H contains the identity.

Hence or otherwise show that if G is finite then only the first among the above conditions is necessary and sufficient for H to be a subgroub.

§ 3 p. 6, § p. 129, Th. 3. p. 134

2. (a) Define a cyclic group. Show that all subgroups of a cyclic group are cyclic.

(b) Define a ring. Give an example of a ring which is not an integral domain.

§ 19 p. 129, Th, 9 p. 146. § 1 p. 168 Ex. 6 p. 193

3. (a) What is a field, and when is it said to be ordered ? Show that the field of rational numbers is ordered.

(b) What is a vector space ? Let V be the set of all (ordered) pairs of real numbers. If $x=(\xi_1, \xi_2)$ and $y=(\eta_1, \eta_2)$ are elements of V, write

$$x+y=(\xi_1+\eta_1.\ \xi_2+\eta_2)$$
$$\alpha x=(\alpha_1\xi,\ 0),\ \alpha \text{ is a scalar}$$
$$0=(0.\ 0)$$
$$-\alpha=(-\xi_1,-\xi_2).$$

Is V a vector spaee with respect to these definitions of the operations ? Why ?

§ 6 p. 195, § 15 p. 224, § 2 p. 285, Refer d p. 295

Kanpur 1971

1. (a) State and prove the distributivity law of union over intersection of sets

(b) Define a composiie mapping. Give one example. Show by means of an example that the two mappings defining a composite mapping are not commutative.

See set Theory,

2. (a) For a *group* $(G,.)$ prove that

$$\forall\ a, b \in G \Rightarrow (a.b)^{-1}=b^{-1}.a^{-1}.$$

(b) Define the order of an element belonging to a *group* and prove that :—

(i) the order of every element of a finite *group* is finite,

(ii) the order of an element of a *group* always equals the order of its inverse.

$$\forall\ a, b \in G \Rightarrow (a.b)^{-1}=b^{-1}.a^{-1}.$$

Prop 9 p. 49. § 12 p. 79, Th. 9 p. 81, Th. 11 p. 82,

3. (a) Define a *ring*. Give one example each of a commutative and non-commutative rings.

(b) Show that the set of Gaussian-integers

$S=\{x : x=a+ib,\ a, b \in I\}$ where I is the set of integers, is an *integral domain.*

Universlty Paper

§ 1 p. 168, Ex. I (a) p. 169, Ex. 3 p. 172, Ex. 5 p. 199

4. (a) Give set theoretic definition of a complex number and prove that set of all complex numbers is a *field* under addition and multiplication of complex numbers.

(b) Define a *vector space* over a given *field*. Give one example and justify it.

Proceed as in Ex 2 p. 170, § 2 p. 285, Ex. 2 p. 287

5. Fill in the blanks in the following statements in order to make them mathematically meaningful :—

Example : In a group $(G, +)$ if every two elements $a, b \in G$ are such that $a+b=b+a$, then G is called *an Abelian group*. (Horizontal short lines indicate blanks).

(*i*) In general a conic can be made to pass through — — —points lying in the plane of the conic.

(*ii*) A commutative ring with no zero divisors is called — — —.

(*iii*) A commutative division ring is called — — —.

(*iv*) A one-one onto mapping which preserves group operation is called — — —.

(*v*) A ring (R, +, .) whose non-zero elements form a group under multiplication is called — — —.

Give Isomorphism, Field.

Rajasthan 1971

1. (a) Let $(a, b) \sim (c, d)$ iff $a+b=d+c$, where a, b, c, d are natural numbers, then show that $\sim$ is an equivalence relation defined on $N \times N$.

(b) Define semi-group and group. Show that a non-void semi-group G is a group if for any $a, b, \in G$, equations $ax=b$ and $ya=b$ have solutions.

See Set Th. See p. 7, Grop 10 p. 50

3. (a) Define a sub-group. Show that the intersection of any two sub-group is a sub-group.

(b) Define a cyclic sub-group. Prove that the order of a cyclic sub-group is equal to the its generator.

§1 P. 129, § 4 p. 140, Th. 9 P.146

4. (a) Express the permutation $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 4 & 1 & 2 & 6 \end{pmatrix} \in S_6$ as the product of disjoint cycles. State whether P is even or odd permutation. Also give its order.

(b) What do you understand by :
(i) Homomorphism from group G into group G'
(ii) Group G is isormorphic to group G'.
If e and e' be the identity of groups G and G' respectively and f be homomorphism from G to G', show that
(i) $f(e)=e'$ and
(ii) $f(a^{-1})=[f(a)]^{-1}$, $a \in G$.
see p. 61, § 16 p. 94, § 1 p 431, § 4 p 432

5. (a) Define :
(I) a ring with unity,
(ii) Zero civisors in a ring.

Prove that if a non-zero element x of a ring R with unity has a multiplicative inverse then x cannot be a zero-divisor.

(b) What do you mean by an ideal in a ring ? Show that if U be an ideal in a ring R with unity 1 such that $1 \in U$, then $U=R$
§ 3 p. 177, § 20 p. 245, Th. 22 Th. 252

6. (a) For any real numbers a. b, we define
$$a+b=a+b-1 \text{ and } a \times b=a+b-ab,$$
then show that $[R, +, \times]$ is a field What are the additive and multiplicative identity of this field ?

(b) What do you mean by the characteristic of a field ? Give examples of a field with zero characteristic and a field with characteristic 5.
Q. 7 p. 188, See Note p. 255

Karnatak 71

1. (a) Do the set I of all integers form a group w.r.t. the binary operatian * defined by
$$a * b=a+b+1 \text{ ?}$$

(b) Let G be a group and S be a non-empty sub-set of G. Then S is a subgroup of G iff
(i) $\forall\ a, b \in S \Rightarrow ab \in S$,
(ii) $\forall\ a \in S$, the inverse a^{-1} of a is in S.
Q. 15 (c) p 21, Th. I p. 131

2. (a) Every subgroup H of a cyclic group G generated by a is cyclic.

(b) Let N be a normal subgroup of a group G. Then

University Paper

Then the map $f : G \to G/N$ of G into the quotient group G/N defined by $f(x) = x\,N \;\forall\; x \in G$ is a homomorphism of G onto G/N and the kernel of f is N.

Th. 9 p. 146 Th. 4 p 435

3. (a) Let a be an element of a commutative ring R with unity. Then the set $M = \{ra : r \in R\}$ is an ideal in R. Further M is the smallest ideal in R which contains a.

(b) Prove that the set M of 2×2 matrices over the field of real numbers is a ring w. r. t. matrix addition and multiplication.

Th. 25 p. 257, Q. 3 p. 172

4. (a) Let C be the set of the ordered pairs (a, b) of real numbers. Addition and multiplication in C are defined by the equations

(i) $(a, b)+(c, d)=(a+c, b+d)$.

(ii) $(a, b)\,(c, d)=(ac-bd, bc+ad)$.

Prove that C is a field.

(b) Prove that the set of numbers of the form $a+b\sqrt{2}$ with a and b as integers is an integral domain w.r.t. ordinary addition and multiplication.

Q. 8 p. 202, Q. 5 p. 193.

Gorakhpur 72

1. (a) Define a group. Examine whether the set of all rational numbers, other than 1, with binary operation defined by $a \,0\, b = a + b - ab$, is a group or not.

(b) Define the order of an element of a group. Prove that the elements a and a^{-1} in a group are always of the same order.

§ 3 p. 6, Q. 15 (a) p. 20, § 12 p. 79, Th 11 p. 82

2. Define a sub group. Show that the set of all elements 'a' of a group G such that $a\,x = x\,a$ for every element x of G is a sub-group of G.

Prove that every sub-group of a cyclic group is itself a cyclic group.

§ 1 p. 129, Ex. 2 p. 136, Th. 9 p. 146

3. (a) Name a group which is isomorphic to the group of numbers 1, i, −1, −i and set up an isomorphism between the two groups.

(b) Prove that every cyclic group of infinite order is isomorphic to the additive group of the ring of integers.

Q. 2 p. 118, Th. 21 p. 124

4. (a) Define an integrers domain. Give an example of an integral domain.

Do the set of odd integers form an integral domain ? Give reasons in support of your answer.

(b) Show that the set of all even integers from a commutative ring without unity.

§ 5 p. 192 See 6 p. 193, no, Then do not form even a group. See 4 p. 10

5. (a) Define a field. Show that an integral domain with a finite number of elements is necessarily a field.

(b) Using natural definitions of addition and scalar multiplication, examine whether the set of all polynomials of degree greater than five over a field F is a vector space over that field or not.

§ 6 p. 195, Th. 4 p. 206, Q. 5 p. 292

Indore 72

1: (a) If a permutation P be expressed as a product of a transpositions and also as a product of b transpositions, show that either both a and b are even or both are odd, that is, $a \equiv b \pmod 2$.

(b) Prove that the numbers, 1, i, $p-1$, −i, where $i=\sqrt{-1}$ form an abelian group with resqect to ordinary multiplication. Write the multiplication table.

Th. 7 p. 67, Q. 9 p. 15.

2. (a) Prove that, of the $\lfloor n$ permutations on n symbols $\lfloor n/2$ are even and $\lfloor n/2$ are odd and also that the $\lfloor n/2$ even permutations form a group with respect to permutation multiplication.

(b) Show that the *n th* roots of unity form a multiplicative cyclic group.

§ 10, p. 70, Th. 8 p. 71, Q. I p. 121.

3. (a) Prove that every finite group G is isomorphic to a permutation group.

(b) If Q be the additive group of rational numbers and Z the sub group of integers, what are the cosets of Z in Q ?

Th. 17 p. 114, Refer Q. 4 p. 150.

4. (a) Show that, it is possible to construct a field, from the elements of an integral domain I, called the quotient field of the integral domain, which contains a sub-system D of elements isomorphic to the integral domain I.

(b) Prove that the set of all real valued functions of x defined over the closed interval [0, 1] forms a ring with respect to addition and multiplication defined as follows :

$$(f+g)(x) = f(x)+g(x)$$
$$(f.g)(x) = f(x)\ g(x)$$

Prove that it is not an integral domain.

See p. 242 C, D, E p. 238, 239, Q. 6 p. 174.

Rajsthan 1972

1. (a) Let the relation R in the set of real numbers be defined as $a\,R\,b$ if and only if $1+ab>0$. Show that the relation is reflexive and symmetric but not transitive.

(b) If an element a of group G is of order n, and p is prime to n, then show that a^p is also of order n.

See my book on set theory. Th. 14 p. 84.

2. (a) Show that the product HK of two sub-groups H, K of a group G is a sub-group of G, if and only if HK = KH.

(b) Show that the multiplicative group

$$G=\{1, \omega, \omega^2\}$$

is isomorphic to the permutation group

$$G'=\{I, (a\ b\ c),\ a\ c\ b)\}$$ on three symbols a, b, c

Th. 8 p. 145, Q. 12 p. 104.

3. (a) Show that every finite group of prime order must be cyclic.

(b) Define automorphism of a group. Show that the set of all automorphism of a group forms a group with respect to composite of functions as the composition.

Cor. 4 p. 163, Th. 6 p 443.

4. (a) A ring R is without zero-divisors, if and only if the cacellation law holds in R.

(b) Prove that, if m is a fixed integer, the set P of integers given by

$$P=\{xm : x \text{ is an integer}\}$$

is an ideal of the ring R of all integers.

Th. I p. 192, Q. 3 p. 249.

5. (a) Show that every prime field of characteristic zero is isomorphic to $(Q,+,\cdot)$, the quotient field of the integral domain of integers.

(b) If a ring R is an integral domain, show that so is the R $[x]$, the polynomial ring over the ring R,

Th. 7 p.466 § 28 p. 268

Karnatak 72

1. (a) Define an Abelian group.

Prove that the set of all $m \times n$ matrices over the set of integers is an Abelian group with matrix addition as composition.

(b) Prove : the group $(\{a, a^2, \ldots\ldots a^n\}, .)$ is a cyclic group of order n generated by a.

§ 3 p. 67, Ex 11 p. 17, Th. 19 p. 120.

2 (a) Define the Isomorphism of groups.

Let $f : G \to G'$ be an isomorphism and e, e' are respectively the identities in G, G'. Then prove that $f(e)=e'$.

(b) If H is a normal subgroup of a group G, then prove that

(i) for every pair of cosets Ha and Hb

$$Ha\ Hb=Hab$$

(ii) The cosets of H in G form a group w.r.t multiplication of subsets of a group.

§ 16 p. 94, § 17·1 p. 108, Th. 3 p. 405, Th. 12 p. 424

3. (a) Every homomorphic image of a group G is a isomorphic with some quotient group thereof. Conversely every quotient group of a group is a homomorphic. Prove this,

(b) If p is an arbitrary element of a commutative ring R, then prove that $P=\{p.r : r\in R\}$ is an ideal in R.

Th. 4, 5 p 435, 36, Th. 25 p. 257.

4. (a) Prove that a commutative ring R with unity is an integral domain iff $\forall\ a, b, x \in R$ with $x\neq 0$, $ax=bx \Rightarrow a=b$.

(b) Prove that everp finite integral domain is a field.

Th. I p. 192, § 5 p. 192 (c) p. 193, Th. 4 p. 206.

Kanpur 72 M.Sc. not B.Sc.

1, (a) Explain the isomorphism of groups giving an illustration. If a group G is isomorphic to G' show that

(i) the image of the identity of G is the identity of G' and

(ii) the image of the inverse of an element $a\epsilon G$ is the inverse of the image of a.

(b) Prove the every finite group G is isomorphic to a permutation group.

§ 16 p. 94, § 17 p. 108 Th. 17 p. 114.

2. If H_1 and H_2 are two sub-groups of a group G, show that $H_1 \cap H_2$ is also a sub-group of G.

Prove that the product $H_1 H_2$ of two sub-groups of a group is sub-group iff

$$H_1H_2=H_2H_1.$$

§ 4 p. 140, Th. 8 p. 145.

3. Define the quotient group. If H be a normal sub-group of a group G and K a normal sub-group of G containing H then

$$G/K\cong G/H/K/H.$$

See p. 425.

4. What do you mean by an automorphism of a group ? Show that the set of all inner automorphisms of a group G is a sub group of the group of its automorphism isomorphic to the quotient group G/Z of G relative to the central Z.

§ 4 p. 442, Th. 8 p. 447.

5. Prove that every homomorphic image of a ring is isomorphic to some residue class ring thereof and conversely every residue class ring of a ring is a homomorphic image of the ring.

Th. 4 p. 464, Th. 6 p. 465

6. (a) Give the definition of a field and show that a field has no proper ideals.

(b) Show that the left ideal generated by the union $I_1 \cup I_2$ of two left ideals is the set $I_1 + I_2$ consisting of the elements of the ring R obtained on adding any element of I_1 to any element of I_2.

§ 6 p. 195, Th 20 p. 251, Q I p. 253.

7. If A is an integral domain, prove that the polynomial ring A [x] is also an integral domain.

If f(x) and $g(x) \neq 0$ be any two polynomials over a field F, show that $\exists$ unique polynomials q(x) and r(x) over F such that $f(x) = g(x)\, q(x) + r(x)$ where r(x) is either zero or of a degree less than that of g(x).

§ 28 p. 268, § 30 p. 272

8. (a) Define a linearly independent system of vectors and show that each sub-space W of a vector space V(K) of dimension n is a finite dimensional space with dimension $\leq n$.

(b) Show that if W is a sub-space of dimension m of a vector space V(K) of dimension n then the dimension of the quotient space V/W is $n-m$

p. 320, Th 23 p. 344, Th. 29 p. 355

9 Define the dual space of a vector space and show that the dual space V* of a space V(K) of finite dimension n is itself of dimension n.

§ 24 p. 389, § 25 p. 394

10. What do you mean by a Galois group ? If L is a finite, separable and normal extension of K then the mapping defined by $M \to G(L/M)$ is a one-one mapping of the set of intermediate fields M between K and L into the set of sub-groups of the Galois group G(L/K) of L over K.